

1  
2  
3  
4  
5  
6  
7                   UNITED STATES DISTRICT COURT  
8                   FOR THE WESTERN DISTRICT OF WASHINGTON  
9                   AT SEATTLE

10 JESUS CASTILLO, MARK KNOWLES, ALEX  
11 RODRIGUEZ, AND NICHOLAS JAMES  
12 THROLSON, individually, and on behalf of  
13 those similarly situated,

14                   Plaintiffs,

15                   v.  
16 COSTCO WHOLESALE CORPORATION, a  
17 Washington corporation,

18                   Defendant.

19                   NO. 2:23-cv-1548

20                   **COMPLAINT - CLASS ACTION**

21                   **JURY TRIAL DEMANDED**

22                   Plaintiffs Jesus Castillo, Mark Knowles, Alex Rodriguez, and Nicholas James Throlson  
23 (“Plaintiffs”), individually and on behalf of themselves and all others similarly situated, by and  
24 through their attorneys of record, assert the following against Defendant Costco Wholesale  
25 Corporation (“Costco” or “Defendant”).

26                   **INTRODUCTION**

27           1. This class action lawsuit arises out of Costco’s unlawful data-sharing practices of  
28 using online third-party tracking technologies, such as Meta Platforms, Inc.’s Pixel Code (“Pixel”  
29 or “Meta Pixel”), to surreptitiously disclose millions of Americans’ private and protected  
30 communications, including their highly personal health information, to third parties, all without  
31 consumers’ knowledge or consent. By purposely embedding and deploying Pixel on Costco’s

1 Website, [www.costco.com](http://www.costco.com), Costco engages in the unauthorized disclosure of its Pharmacy  
 2 patients' highly sensitive Personal Health Information ("PHI") and Personally Identifiable  
 3 Information ("PII") (collectively "Sensitive Information") to third parties, including Meta  
 4 Platforms, Inc. d/b/a Meta ("Facebook").<sup>1</sup> Such conduct blatantly violates state and federal law.

5       2. As a multinational company, and one of the largest global retailers today,  
 6 Defendant operates a membership-only warehouse club that serves millions of customers  
 7 worldwide.<sup>2</sup> Defendant owns and controls the website [www.costco.com](http://www.costco.com) and the subpages for its  
 8 pharmaceutical immunization services provided by Costco Pharmacy at  
 9 [www.costco.com/pharmacy](http://www.costco.com/pharmacy) (collectively Defendant's "Website"). In its ordinary course of  
 10 business, Defendant encourages patients and prospective patients to use its Pharmacy subpages  
 11 of its Website, so patients and prospective patients can communicate about their prescriptions,  
 12 research medications for purchase, order new prescriptions, request refills for existing  
 13 medications, inquire about specific immunizations, search for local Medicare supplemental  
 14 insurance, and more. In doing so, Costco represents to patients that its Website, which includes  
 15 its Pharmacy webpages, is a secure platform and that the information provided therein will  
 16 remain protected and confidential. Yet, Costco fails to disclose or omits the fact that it shares  
 17 patient online activities and personal health information with Meta via Pixel.

18       3. Recently, Plaintiffs became aware that Defendant incorporates online tracking  
 19 technologies, such as Pixel, on its Website and the Pharmacy subpages. Pixel is a snippet of code  
 20

---

21 <sup>1</sup> At all relevant times, Costco is and was a "covered entity" under HIPAA because it is "[a] health care provider  
 22 who transmits any health information in electronic form in connection with a transaction covered" by HIPAA. 45  
 23 C.F.R. § 160.103. A HIPAA "health care provider" is "a provider of medical or health services" and "any other  
 24 person or organization who furnishes, bills, or is paid for health care in the normal course of business." *Id.* Moreover,  
 25 "health care" is defined under HIPAA as "care, services, or supplies related to the health of an individual" and  
 26 includes "[p]reventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling,  
 service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an  
 individual or that affects the structure or function of the body; and . . . [the s]ale or dispensing of drug, device,  
 equipment, or other item in accordance with a prescription." *Id.* Costco provides care, services, and supplies related  
 to the health of an individual, which includes Costco Pharmacy and its sale and dispensing of prescription  
 medications to patients and prospective patients.

<sup>2</sup> *Company Report: Costco Wholesale Corp., Company Overview*, Bloomberg Law (Aug. 21, 2023).

1 that, when embedded on a website, tracks the website visitor's activity on that website and sends  
 2 that data to a third party, like Meta. This includes tracking and logging pages and subpages the  
 3 website user visits during a website session that reveal patient status and other personal  
 4 identifying and protected health information, clicks, searches, and other submissions to the  
 5 website, which in many cases includes sensitive personal and identifying information that is not  
 6 anonymized. Indeed, Pixel is routinely used to target specific customers by utilizing the data  
 7 gathered through Pixel to build profiles for the purpose of future targeting and marketing. Here,  
 8 the information transmitted to third-party Meta, without Plaintiffs' consent, most certainly  
 9 included private health information,<sup>3</sup> which is some of the most personal and sensitive data  
 10 Plaintiffs have.

11       4.     Additionally, when a patient communicates with Costco's Website where Pixel is  
 12 present, Pixel source code causes the exact content of the patients' communications with the  
 13 Website to be re-directed to Meta in a fashion that identifies the person as a patient. For example,  
 14 Plaintiffs are patients and prospective patients of Costco Pharmacy and, while receiving or  
 15 researching pharmaceutical care from Costco Pharmacy, used the Website to communicate about  
 16 ordering new prescriptions; requesting prescription refills; enrolling in automated prescription  
 17 services; viewing prescription history, new prescriptions, and prescription pricing; and  
 18 conducting medication-related research. Unbeknownst to Plaintiffs and Class Members, when  
 19 they attempted to log-in to their patient accounts, searched for prescriptions and related pricing,  
 20 and inquired about immunizations, among other sensitive health-related topics, Pixel secretly  
 21 intercepted, recorded, and transmitted those private communications to Meta.

22

23

24

25

26

---

<sup>3</sup> Under HIPAA, "health information" is defined as "any information[], whether oral or recorded in any form or medium, that . . . [i]s created or received by a health care provider . . . and [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Additionally, HIPAA defines "health care" as "care, services, or supplies related to the health of an individual" and includes, but is not limited to, the "[s]ale or dispensing of drug, device, equipment, or other item in accordance with a prescription." *Id.*

1       5.     Defendant's use of Pixel allows for a broad scope of patient information,  
 2 including highly confidential health information, to be collected and transmitted to Meta without  
 3 patients' knowledge or consent. Specifically, Pixel is designed to track website users' activity on  
 4 a website or application. It can capture how visitors interact with the site, including buttons they  
 5 click and information they provide to form fields or otherwise. These are collectively known as  
 6 "Website Communications."

7       6.     Furthermore, Defendant uses Pixel to improve and save costs on its marketing  
 8 campaigns, improve its data analytics to increase revenue by, among other things, attracting new  
 9 patients and improving its services for existing patients. Defendant also uses Pixel to gain insight  
 10 into patients, through secret tracking, that it could not otherwise have or use.

11      7.     Here, Defendant solicited and obtained Plaintiffs' and the Class's Sensitive  
 12 Information as a health care provider. Specifically, Defendant used the Sensitive Information to  
 13 gain additional insights into its patients and prospective patients, improve its return on its  
 14 marketing dollars, and ultimately, to increase revenue. Costco encouraged Plaintiffs and the Class  
 15 Members to access and use its Website for the purpose of receiving health care services or  
 16 obtaining health-related information and knowledge, including receiving pharmaceutical  
 17 services.<sup>4</sup>

18      8.     As a result of Defendant's use of Pixel, Plaintiffs' and the Class's Sensitive  
 19 Information, including, but not limited to, computer IP addresses; patient status; prescription  
 20 information (including specific drugs and pricing information); immunization information;  
 21 treatments; patient location; health insurance coverage; and unique identifiers used to link  
 22 Plaintiffs' and the Class's private communications via the Website to their Facebook accounts,  
 23 was compromised and disclosed to third parties without authorization or consent.

---

24  
 25  
 26     <sup>4</sup> See *Create an account*, <https://mobilecontent.costco.com/live/resource/img/pharmacy-training/pharmacy-training.html#/lessons/w-E1ac5YoS4RPxcoQgAASNxFz9k6pcgN> (last visited Aug. 30, 2023) (encouraging patients to sign up for the Costco Mail Order option so that they can, "Fill your prescriptions online and have it mailed to your home.").

1       9. Such private information would allow Meta to know that a specific patient was  
 2 seeking confidential pharmaceutical care or exploring drug therapy options for a specific  
 3 condition.

4       10. Plaintiffs and the Class Members never consented to, authorized, or otherwise  
 5 agreed to allow Defendant to disclose their Sensitive Information to anyone other than those  
 6 reasonably believed to be part of Costco, acting in some healthcare-related capacity. Despite this,  
 7 Defendant knowingly and intentionally disclosed Plaintiffs' and the Class Members' Sensitive  
 8 Information to Meta and other undisclosed third parties.

9       11. Plaintiffs and the Class Members also did not consent to the Defendant secretly  
 10 tracking and disclosing their Website Communications and other online user behaviors while on  
 11 Costco's Website.

12       12. Plaintiffs' and the Class Members' exposed Sensitive Information can and will  
 13 likely be further exposed or disseminated to additional third parties.

14       13. As a direct and proximate result of Defendant's unauthorized exposure of  
 15 Plaintiffs' and the Class Members' Sensitive Information, Plaintiffs and the Class Members have  
 16 suffered injury including an invasion of privacy; conversion of their private and valuable personal  
 17 health information for defendant's gain; loss of the benefit of the bargain Plaintiffs and the Class  
 18 Members considered at the time they bargained for pharmaceutical services and agreed to use  
 19 Defendant's Website for services; statutory damages; and the continued and ongoing risk to their  
 20 Sensitive Information.

21       14. As such, Plaintiffs bring this action individually, and on behalf of a Class of  
 22 similarly situated individuals, to recover for harms suffered and assert the following claims:  
 23 Violations of Electronic Communications Privacy Act ("ECPA") (18 U.S.C. § 2511); Violations  
 24 of the Washington Privacy Act (Wash. Rev. Code § 9.73.030 *et seq.*); Violations of the  
 25 Washington Consumer Protection Act ("WCPA") (Wash. Rev. Code § 19.86 *et seq.*); Violations  
 26

1 of the Washington Uniform Health Care Information Act (“UHCIA”) (Wash. Rev. Code. § 70.02  
 2 *et seq.*); Invasion of Privacy; Breach of Implied Contract; Conversion; and Unjust Enrichment.

3 **PARTIES**

4 15. **Plaintiff** Jesus Castillo is a natural person domiciled in the State of California. At  
 5 all relevant times, he resided in South El Monte, California. For the last several years, and most  
 6 recently in 2022, he visited Defendant’s Website while residing in California to transfer his  
 7 prescription medications from another pharmacy to Costco Pharmacy to purchase and refill his  
 8 prescriptions with Costco.<sup>5</sup> He communicated personal, private, and highly sensitive information  
 9 while visiting Defendant’s Website. At all relevant times, Plaintiff J. Castillo had a Facebook  
 10 account and generally remained logged into his account.

11 16. **Plaintiff** Mark Knowles is a natural person domiciled in the State of California.  
 12 At all relevant times, he resided in Redondo Beach, California. For the last six years, and most  
 13 recently in 2023, he visited Defendant’s Website while residing in California to enroll in Costco’s  
 14 mail-in prescription order option; to order, view, and schedule monthly prescription refills; and  
 15 to search for prescriptions and prescription pricing, including by utilizing the Website’s “search”  
 16 bar. He also visited Defendant’s Website to use the patient portal to order new prescriptions and  
 17 request prescription refills. He communicated personal, private, and highly sensitive information  
 18 while visiting Defendant’s Website. At all relevant times, Plaintiff M. Knowles had a Facebook  
 19 account and generally remained logged in to his account.

20 17. **Plaintiff** Alex Rodriguez is a natural person domiciled in the State of California.  
 21 At all relevant times, he resided in Madera, California. For the last several years, and most  
 22 recently in 2023, he visited Defendant’s Website while residing in California to order and view  
 23 new prescriptions and search for prescriptions and prescription pricing, including by utilizing the  
 24 Website’s “search” bar. He also visited Defendant’s Website to use the patient portal to order

25 \_\_\_\_\_  
 26 <sup>5</sup> Further details regarding any Plaintiffs’ medical conditions and prospective or actual medical treatments entered  
 or searched on Defendant’s website are not required to be pled under Fed. R. Civ. P. 8, and doing so would require  
 Plaintiffs to publicly disclose private and sensitive medical data, compounding Defendant’s violation of their  
 medical privacy.

1 new prescriptions, request prescription refills, review co-pay information, review prescription  
 2 pickup times, and communicate with pharmacists and technicians. He communicated personal,  
 3 private, and highly sensitive information while visiting Defendant's Website. At all relevant  
 4 times, Plaintiff A. Rodriguez had a Facebook account and generally remained logged in to his  
 5 account.

6       18.     **Plaintiff** Nicholas James Throlson is a natural person domiciled in the State of  
 7 California. At all relevant times, he resided in Rialto, California. For the last two years, and most  
 8 recently in 2023, he visited Defendant's Website while residing in California to enroll in,  
 9 schedule, and view automatic prescription refill pickup and search for prescriptions and  
 10 prescription pricing, including by utilizing the Website's "search" bar. He also visited  
 11 Defendant's Website to use the patient portal to search for new prescriptions, review prescription  
 12 pricing, and assess whether to request prescription refills through Costco Pharmacy. He  
 13 communicated personal, private, and highly sensitive information while visiting Defendant's  
 14 Website. At all relevant times, Plaintiff N. J. Throlson had a Facebook account and generally  
 15 remained logged in to his account.

16       19.     Plaintiffs reasonably expected that their online communications with Defendant  
 17 were between them and Defendant and that such communications would not be shared with third  
 18 parties without their consent.

19       20.     It is some Plaintiffs' recollection that after using Defendant's Website, they  
 20 received some targeted advertisements related to information they had submitted to Defendant  
 21 via Defendant's Website.

22       21.     **Defendant** Costco Wholesale Corporation is a Washington corporation, is  
 23 licensed to do business in the State of Washington, and has its principal place of business in  
 24 Issaquah, Washington. Defendant's registered agent is John Sullivan, located at 999 Lake Drive,  
 25 Issaquah, Washington, 98027-8990.

22. Defendant is a multinational retailer that operates a membership-only warehouse club. With a corporate history that dates to 1976,<sup>6</sup> Defendant is one of the largest retailers in the world today, with more than 300,000 employees and serving millions of members and non-members around the globe.<sup>7</sup> Defendant sells food, automotive, supplies, toys, hardware, sporting goods, jewelry, electronics, apparel, health, and beauty aids, as well as other goods.<sup>8</sup> Costco also offers pharmaceutical services through the Costco Pharmacy and the Pharmacy webpage.

23. Costco Pharmacy provides online pharmaceutical services to patients and prospective patients, which include prescription refills, immunization scheduling, home delivery, Medicare plan finder, warehouse pickup options, customer service, fulfilling new prescription orders, information about health and wellness clinics, fulfilling pet medications, free language translation services available at all Costco pharmacies, and customer service support.<sup>9</sup>

## **JURISDICTION AND VENUE**

24. This Court has subject matter jurisdiction over this action under 28 U.S.C. §1332(d)(2)(A) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000.00, exclusive of interest and costs, there are 100 or more members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

25. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because this Complaint asserts claims pursuant to Defendant's violations of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511.

<sup>6</sup> Robert Lewis, *Costco*, Britannica, <https://www.britannica.com/topic/Costco> (last visited Sept. 15, 2023).

<sup>7</sup> *About Us*, Costco Wholesale, <https://www.costco.com/about.html> (last visited Sept. 15, 2023); *Company Profile*, Costco Wholesale, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 15, 2023).

<sup>8</sup> About Us, Costco Wholesale, <https://www.costco.com/about.html> (last visited Sept. 15, 2023); Overview of Costco Wholesale Corp (COST US Equity), Bloomberg Law, <https://www.bloomberglaw.com/company/ticker/COST%20US%20Equity> (last visited Sept. 15., 2023); Costco, Wikipedia, [https://en.wikipedia.org/wiki/Costco#See\\_also](https://en.wikipedia.org/wiki/Costco#See_also) (last visited Sept. 15, 2023); Company Profile, Costco Wholesale, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 15, 2023).

<sup>9</sup> See Costco Pharmacy, [www.costco.com/home-delivery](http://www.costco.com/home-delivery) (last visited Sept. 15, 2023).

1       26. This court has supplemental jurisdiction over Plaintiffs' state law claims under 28  
 2 U.S.C. § 1337.

3       27. This Court has general personal jurisdiction over this action because Defendant is  
 4 a Washington corporation with its principal office located at 999 Lake Drive, Issaquah,  
 5 Washington 98027.

6       28. This Court also has specific personal jurisdiction over this action because the acts  
 7 and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District. At all  
 8 relevant times, Defendant knew its practices would directly result in the collection of information  
 9 throughout the United States and its territories while individuals interacted with Costco's  
 10 Website. Defendant chose to avail itself of the business opportunities by making Costco  
 11 Pharmacy and its services specifically available in the state of Washington and by collecting real-  
 12 time data from website visit sessions initiated by Costco's customers located throughout the  
 13 United States, including in Washington, and the claims alleged herein arise from those activities.

14       29. Costco also knows that many patients and prospective patients visit and interact  
 15 with Costco Pharmacy's webpages while they are physically present in Washington and  
 16 throughout the United States and its territories. Both desktop and mobile versions of Costco's  
 17 Website allow a user to search for nearby Costco warehouses to schedule appointments for  
 18 immunizations and vaccinations,<sup>10</sup> enroll in prescription refill pickup at limited Costco Pharmacy  
 19 warehouse locations,<sup>11</sup> enroll in direct-mail prescription delivery,<sup>12</sup> search pricing and  
 20 information regarding prescription and over-the-counter medications,<sup>13</sup> and locate nearby

---

21  
 22  
 23       <sup>10</sup> *Immunizations*, Costco Pharmacy, <https://www.costco.com/pharmacy/adult-immunization-program.html> (last  
 24 visited Aug. 22, 2023).

25       <sup>11</sup> *Costco RX Locker: Prescription Pickup*, Costco Pharmacy, chrome-  
 26 extension://efaidnbmnnibpcajpcgkclefindmkaj/https://mobilecontent.costco.com/live/resource/img/static-us-  
 landing-pages/pharmacy\_pickup.pdf (last accessed Aug. 22, 2023); *Refill Now*, Costco Pharmacy,  
<https://costco.web.medrefill.com/csweb/#/refill> (last visited Aug. 22, 2023).

27       <sup>12</sup> *About Prescription Mail Order*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html>  
 28 (last visited Aug. 22, 2023); Costco Pharmacy, <https://mobilecontent.costco.com/live/resource/img/pharmacy-training/pharmacy-training.html#/lessons/w-E1ac5YoS4RPxcoQgAASNXFz9k6pcgN> (last visited Aug. 22, 2023).

29       <sup>13</sup> *Member Prescription Program*, Costco Pharmacy, <https://www.costco.com/cmpp> (last visited Aug. 22, 2023).

Medicare insurance<sup>14</sup> by providing the user’s “current location,” or by selecting “my warehouse” and “my delivery location,” as furnished by the location-determining tools of the device the user is using, by the user’s IP address (*i.e.*, without requiring the user to manually input an address), or by a user’s manual entry.<sup>15</sup>

30. Through its Website, which included Pixel tracking technology and was accessible to all Washington residents, Costco allowed consumers to view and interact with its marketed and advertised pharmaceutical services, directly engage with those services, exchange communications with the retailer, and create online accounts. Thus, users' employment of automatic location services in this way means that Costco is continuously made aware that people located throughout the United States, including in Washington, visit and interact with its Website and services made available by Costco, and that such website visitors are being wiretapped in violation of federal and state law.

31. Venue is proper under 28 U.S.C. §§ 1391(b)(1) – (2) because Defendant's principal place of business is in this District and because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

## **FACTUAL ALLEGATIONS**

## A. Defendant Collected, Maintained, and Stored Sensitive Information

32. Defendant Costco began operating its company in 1976 out of a converted airplane hangar in southern California, serving only small businesses.<sup>16</sup> Today, Costco is one of the world's largest retailers, offering a membership-only warehouse club and operating in more than 800 locations worldwide, with approximately 300,000 employees, while serving millions of members around the globe.<sup>17</sup> This retailer giant has grown to amass total sales exceeding \$222

<sup>14</sup> Medicare Plan Finder, Costco Pharmacy, <https://www.costco.com/pharmacy/medicare.html> (last visited Aug. 22, 2023).

<sup>15</sup> Find a Store, Costco Pharmacy, <https://costco.web.medrefill.com/csweb/#/store> (last visited Aug. 22, 2023).

<sup>16</sup> Company Information: The History of Costco, [www.costco.com/company-information.html](http://www.costco.com/company-information.html) (last visited Sept. 15, 2023).

<sup>17</sup> Company Information: The History of Costco, [www.costco.com/company-information.html](http://www.costco.com/company-information.html) (last visited Sept. 14, 2023); Company Profile, Costco Wholesale, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 14, 2023).

1 billion dollars by fiscal year-end 2022.<sup>18</sup>

2       33. Besides food, automotive, supplies, and hardware, among other goods, Costco  
3 offers pharmaceutical services to members and non-members.

4       34. To obtain pharmaceutical services, individuals, like Plaintiffs and members of the  
5 Class, must provide Defendant with highly sensitive information, including PHI, PII, or both.  
6 Defendant compiles, stores, and maintains the highly valuable and sensitive PHI and/or PII and,  
7 often, through the provision of its services, creates records containing additionally highly  
8 sensitive and valuable data concerning patients' computer IP addresses; patient status;  
9 prescription information (including specific drugs and pricing information); immunization  
10 information; treatments; patient location; health insurance coverage; and unique identifiers used  
11 to link Plaintiffs' and the Class's private communications via the Website to their Facebook  
12 accounts. Defendant serves millions of individuals each year, meaning it creates and maintains a  
13 massive repository of Sensitive Information.

14       35. Defendant tells patients it will keep their Sensitive Information secure and private.  
15 Indeed, Defendant maintains a Privacy Policy, stating, “[R]est assured that here at Costco, we  
16 absolutely respect your right to privacy. Costco collects, uses[,] and shares your personal  
17 information in accordance with Your Privacy Rights.”<sup>19</sup> This Policy further provides that Costco  
18 takes “reasonable and appropriate steps to help protect personal information from unauthorized  
19 access, use, disclosure . . .”<sup>20</sup>

20       36. In its Notice of Patient’s Rights, Defendant confirms that its patients have the  
21 right “[t]o have the patient’s pharmaceutical records maintained in a[] . . . confidential manner.”<sup>21</sup>  
22

---

23       <sup>18</sup> *Company Profile*, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 14, 2023);  
24 *Company Information: The History of Costco*, [www.costco.com/company-information.html](http://www.costco.com/company-information.html) (last visited Sept. 14, 2023).

25       <sup>19</sup> *What is Costco’s Privacy Policy?*, Costco Wholesale, [https://customerservice.costco.com/app/answers/detail/a\\_id/1163/~/what-is-costcos-privacy-policy%3F](https://customerservice.costco.com/app/answers/detail/a_id/1163/~/what-is-costcos-privacy-policy%3F) (last visited Sept. 14, 2023).

26       <sup>20</sup> *Costco Wholesale Corporation Your Privacy Rights (United States and Puerto Rico)*, Costco Wholesale, <https://www.costco.com/privacy-policy.html> (last updated June 20, 2023) (last visited Sept. 14, 2023).

21       <sup>21</sup> *Notice of Patient’s Rights*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html#patient-rights> (last visited on Sept. 14, 2023).

1       37. Costco Pharmacy affirms it “respects [each patient’s] right to privacy” and  
 2 reassures it maintains its “patient profile database separately from other Costco records to  
 3 safeguard the confidentiality of personal pharmacy information.”<sup>22</sup>

4       38. Defendant’s Notice of Privacy Practices<sup>23</sup> acknowledges that Costco is “required  
 5 by law to maintain the privacy and security of [its patients’] PHI.”<sup>24</sup> The Notice further states  
 6 that “[t]o protect the privacy of PHI, [Costco] limit[s] the way PHI is used or disclosed to  
 7 others”<sup>25</sup> and acknowledges Costco’s obligation to “obtain . . . written authorization” before a  
 8 patient’s PHI is used or disclosed for any purpose other than that listed in the Notice, including  
 9 for marketing or “payment in exchange for providing [a patient’s] PHI” to a third party.<sup>26</sup>

10      39. Plaintiffs and the Class Members had a reasonable expectation of privacy and  
 11 relied on Defendant to protect the Sensitive Information provided to it and created by it,  
 12 especially because, pharmacists and other health care practitioners and their facilities are always  
 13 required to maintain confidentiality of patient records, with very limited exceptions. Defendant  
 14 knew or should have known that failing to protect patient information adequately could cause  
 15 substantial harm by exposing patient data to unauthorized third parties, causing a loss of privacy  
 16 and loss of control over patients’ personal information. Moreover, through its various policies,  
 17 Defendant acknowledged its obligation to safeguard sensitive information reasonably against  
 18 unauthorized disclosure of such information to third parties, like Meta.

19  
 20  
 21      <sup>22</sup> *Confidentiality of Personal Pharmacy Information*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html#confidentiality> (last visited Sept. 14., 2023).

22      <sup>23</sup> The Costco Health Centers Notice of Privacy Practices is specific to health information handled by Costco  
 23 Pharmacy as it “applies to PHI created, received, maintained or transmitted by or on behalf of Costco Pharmacies,  
 24 Costco Optical Centers, and Costco Hearing Aid Centers (the ‘Costco Health Centers’).”

25      <sup>24</sup> *Costco Health Centers Notice of Privacy Practices* (Jan. 1, 2019), at 1, chrome-extension://  
 26 efaidnbmnnibpcajpcgclefindmkaj/https://www.costco.com/wcsstore/CostcoUSBCCatalogAssetStore/rx/HIPAA-  
 27 Privacy-Practice-19.pdf (last visited Sept. 14, 2023). Costco’s Notice provides that PHI relates to (1) a patient’s  
 28 physical or mental condition, (2) the provision of health care services to the patient, or (3) payment for a patient’s  
 29 health care, and that this could include a patient’s “prescriptions” and “information [] provide[d] on any Costco  
 30 Health Center patient health history form.” *Id.*

31      <sup>25</sup> *Id.*

32      <sup>26</sup> *Id.* at 4.

1       40. A privacy violation of this type, in which Defendant intentionally granted access  
 2 to third-party Meta to record and collect information on the company's systems, collect user data,  
 3 including Sensitive Information and highly confidential medical records without restriction,  
 4 could not occur but for Defendant's blatant disregard for patient privacy.

5       41. Defendant violated several basic privacy and data standards regarding patient  
 6 privacy and confidentiality.

7       42. As described throughout this Complaint, Defendant did not reasonably protect,  
 8 secure, or store Plaintiffs' and the Class Members' Sensitive Information, but rather intentionally  
 9 and knowingly granted Meta access to confidential information that it knew or should have  
 10 known was unlawful.

11       43. Defendant deprived Plaintiffs and the Class Members of their privacy rights when  
 12 it (i) installed Meta Pixel on its Website and thereby surreptitiously tracked, recorded, and  
 13 disclosed Plaintiffs' and other online patients' personal and private communications and  
 14 information; (ii) disclosed Plaintiffs' and the Class Members' protected information to Meta—  
 15 an unauthorized third party; and (iii) and undertook this pattern of conduct without notifying—  
 16 and without obtaining the express written consent of—Plaintiffs and the Class Members.

17       44. Consequently, Meta, and potentially other third parties, obtained access to and  
 18 collected confidential patient data without the patients' authorization, resulting in a significant  
 19 invasion of patient privacy and disclosure of sensitive data.

## 20       B. The Meta Pixel

21       45. Through its Website, Defendant connects Plaintiffs and the Class Members to  
 22 Defendant's digital health care platform with a core goal of increasing profitability.

23       46. In furtherance of that goal, and to increase the success of its advertising and  
 24 marketing, Defendant purposely embedded and deployed Meta Pixel on its Website. By doing  
 25 so, Defendant surreptitiously shares its patients' and prospective patients' identities and online  
 26 activity, including private communications and search results related to past and current

1      prescription medications, treatments, immunizations, health insurance coverage, and other  
 2 Sensitive Information, with Meta.

3        47. It is no surprise that Meta's core business function is to sell advertising; it does so  
 4 on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars  
 5 in annual revenue comes from advertising—a practice in which Meta actively participates by  
 6 using algorithms that approve and deny ads based on the ads' content, human moderators that  
 7 further review ads for both legality and aesthetics prior to and after the ads are published, and  
 8 other algorithms that connect ads to specific users, without the assistance or input of the  
 9 advertiser.

10        48. Over the last decade, Facebook, now Meta, has become one of the largest and  
 11 fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily,  
 12 monthly, and annual user base has grown exponentially to billions of users.

13        49. Meta's advertising business has been successful due, in significant part, to Meta's  
 14 ability to target users, both based on information users provide to Meta, and based on other  
 15 information about users Meta extracts from the Internet at large. Given the highly specific data  
 16 used to target particular users, thousands of companies and individuals utilize Facebook's  
 17 advertising services.

18        50. One of Meta's most powerful advertising tools is the "Meta Pixel" (formerly the  
 19 "Facebook Pixel"), which it first launched in 2015.

20        51. Meta branded Pixel as "a new way to report and optimize for conversions, build  
 21 audiences and get rich insights about how people use your website." Meta further stated:

22        Facebook pixel, [is] a new way to report and optimize for conversions, build  
 23 audiences[,] and get rich insights about how people use your website. We're also  
 24 announcing the availability of custom conversions, a new rule-based method to  
 track and report conversions for your Facebook ads.

25        Facebook pixel makes things simple for advertisers by combining the  
 26 functionality of the Conversion Tracking pixels and Custom Audience pixels into  
 a single pixel. You only need to place a single pixel across your entire website to

1 report and optimize for conversions. Since it is built on top of the upgraded  
 2 Custom Audience pixel, all the features announced in our previous blog post  
 (Announcing Upgrades to Conversion Tracking and Optimization at Facebook)  
 3 are supported through Facebook pixel as well.

4 [Advertisers and website operators] can use Facebook pixel to track and optimize  
 5 for conversions by adding standard events (*e.g.*, Purchase) to your Facebook pixel  
 6 base code on appropriate pages (*e.g.*, purchase confirmation page).<sup>27</sup>

7 52. Pixel is a publicly available piece of code that Meta makes available to website  
 8 developers for free. Website developers can choose to install and use Pixel on their websites to  
 9 track and measure certain actions, such as clicks, text searches, and page views, including the  
 URLs triggered by page views, by website visitors. When a website visitor takes an action a  
 developer chooses to track on its website, Pixel is triggered and sends data about that “Event” to  
 10 Meta. All of this happens without the user’s knowledge or consent.

11 53. Web browsers are software applications that allow consumers to navigate the web  
 12 and view and exchange electronic information and communications over the Internet. Each  
 13 “client device” (such as a computer, tablet, or smart phone) accesses web content through a web  
 14 browser (*e.g.*, Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser,  
 15 and Microsoft’s Edge browser).

16 54. Every website is hosted by a computer “server” that holds the website’s contents  
 17 and through which the entity in charge of the website exchanges communications with Internet  
 users’ client devices via their web browsers.

18 55. Ultimately, a browsing session online may consist of thousands of web  
 19 communications. Web communications consist of HTTP or HTTPS Requests and HTTP or  
 20 HTTPS Responses, and any given browsing session may consist of thousands of individual  
 21 HTTP Requests and HTTP Responses, along with corresponding cookies:

- 22
- 23     • An **HTTP Request** is an electronic communication a website visitor sends from  
           his device’s browser to the website’s server. There are two types of HTTP  
           Requests: (1) GET Requests, which are one of the most common types of HTTP

---

26     <sup>27</sup> Cecile Ho, *Announcing Facebook Pixel*, Meta (Oct. 14, 2015), <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/> (last visited Sept. 14, 2023).

1 Requests—in addition to specifying a particular URL (*i.e.*, web address), GET  
 2 Requests can also send data to the host server embedded inside the URL, and can  
 3 include cookies; and (2) POST Requests which can send a large amount of data  
 4 outside of the URL. In this case, a patient’s HTTP Request would be asking  
 5 Defendant’s Website to get certain information, such as a list of clinic locations  
 6 or prescriptions.

- 7 • **Cookies** are a text file that website operators and others use to store information  
 8 on the website visitor’s device; these can later be communicated to a server or  
 9 servers. Cookies are sent with HTTP Requests from website visitor’s devices to  
 10 the host server. Some cookies are “third-party cookies,” which means they can  
 11 store and communicate data when visiting one website to an entirely different  
 12 website. Third-party cookies are created by a website with a domain name other  
 13 than the one the user is visiting, in this case Meta.<sup>28</sup> There are also “first-party  
 14 cookies,” like the fbp cookie, which is created by the website the user is visiting,  
 15 in this case Defendant.<sup>29</sup> Meta uses both first- and third-party cookies in Pixel to  
 16 link Facebook IDs and Facebook profiles, and Defendant sends these identifiers  
 17 to Meta.
- 18 • An **HTTP Response** is a response to an HTTP Request. It is an electronic  
 19 communication that is sent as a reply to the website visitor’s device’s web browser  
 20 from the host server. HTTP responses may consist of a web page, another kind of  
 21 file, text information, or error codes, among other data. Basically, the HTTP  
 22 Response is when the website sends the requested information (*see* the HTTP  
 23 Request); this is sometimes called the “Markup.”

---

24  
 25 <sup>28</sup> *Third-Party Cookie*, PCMag.com, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Sept. 14, 2023). This is also confirmable using web developer tools to inspect a website’s cookies and track network activity. This is confirmable by tracking network activity.

26 <sup>29</sup> *First-Party Cookie*, PCMag.com, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Sept. 14, 2023). This is also confirmable using web developer tools to inspect a website’s cookies and track network activity.

1       56. A user's HTTP Request essentially asks the Defendant's Website to retrieve  
 2 certain information (such as "Drug Pricing"). The HTTP Response then renders or loads the  
 3 requested information in the form of Markup (*i.e.*, the pages, images, words, buttons, and other  
 4 features that appear on the patient's screen as they navigate Defendant's Website).

5       57. Every website, including Defendant's, is composed of Markup and "Source  
 6 Code." Source code is a set of instructions that commands the website visitor's browser to take  
 7 certain actions when the web page loads or when a specified event triggers the code.

8       58. Source code may also command a web browser to transmit data to third parties in  
 9 the form of an HTTP Request. Such data transmissions allow a website to export data about users  
 10 and their actions to third parties. Third parties receiving this data are typically configured to track  
 11 user data and communications for marketing purposes.

12       59. Transmission of such data can be done quietly in the background without  
 13 notifying the web browser's user. The pixels are invisible to website users and thus, without any  
 14 knowledge, authorization, or action by the user, the website site developer (or website  
 15 commander) can use its source code to contemporaneously and to invisibly re-direct the user's  
 16 PII and other non-public medical information to third parties. Through Pixel, Defendant uses  
 17 source code that can accomplish just that.

18       60. Pixel "tracks the people and the types of actions they take."<sup>30</sup> According to Meta,  
 19 Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by  
 20 understanding the actions [website visitors] take on [its] website.<sup>31</sup> Thus, by secretly recording  
 21 and transmitting data to Meta—without the user's knowledge or consent—Pixel acts much like  
 22 a traditional wiretap controlled by Defendant.

23       61. Through this online tracking technology, Meta intercepts each page a user visits,  
 24 what buttons they click, as well as the specific information the user inputs into the website and  
 25

---

26<sup>30</sup> *Retargeting*, Facebook, <https://www.facebook.com/business/goals/retargeting> (last visited Sept. 14, 2023).

<sup>31</sup> *About Meta Pixel*, Meta Business Help Center, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Sept. 14, 2023).

1 other searches conducted. Pixel sends each of these pieces of information to Meta with PII, such  
 2 as the user's IP address. Meta stores this data on its own servers, in some instances for years on  
 3 end, and independently uses the data for its own financial gain.

4       62. Importantly, this data is often associated with the individual user's Facebook  
 5 account. For example, if the user is logged into their Facebook account when the user visits  
 6 Defendant's website, Meta receives third-party cookies allowing Meta to link the data collected  
 7 by Pixel to the specific Facebook user. In other words, a user's personal and private information  
 8 sent by the Meta Pixel to Facebook is sent alongside that user's personal identifiers, including IP  
 9 address and cookie values, which can be linked to the user's unique Facebook account.

10      63. Meta accomplishes this by placing cookies in the web browsers of users logged  
 11 into their services, which aids Meta in identifying users.

12      64. One such example is the "c\_user" cookie, which is a type of third-party cookie  
 13 assigned to each person who has a Facebook account. The "c\_user" cookie contains a numerical  
 14 value known as the Facebook ID ("FID") that uniquely identifies a Facebook user. It is composed  
 15 of a unique and persistent set of numbers. A user's FID is linked to their Facebook profile, which  
 16 generally contains a wide range of demographic and other information about the user, including  
 17 pictures, personal interests, work history, relationship status, and other details. Because the user's  
 18 Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any  
 19 ordinary person—can easily use the Facebook Profile ID to quickly, and easily, locate, access,  
 20 and view the user's corresponding Facebook profile. Thus, when a Facebook user visits  
 21 Defendant's Website while logged in to their Facebook account, Pixel transmits the user's private  
 22 web communications with the Defendant along with the "c\_user" cookie. Meta can then use this  
 23 information to match the web communications with the user's Facebook ID.

24      65. Even if a user does not have a Facebook account or is not logged in to Facebook  
 25 when browsing the Defendant's Website, Pixel transmits the user's web communications with  
 26 Defendant's Website to Meta along with a unique identifier associated with another cookie called

1 the “\_fbp” cookie. Meta can then use that unique identifier to link the user’s web communications  
 2 with the user’s Facebook ID. And if a user who does not have a Facebook account later creates  
 3 an account, Meta may be able to associate the user’s historical browsing history intercepted via  
 4 Pixel and “\_fbp” cookie to the newly created account.

5       66. Judge William H. Orrick on the U.S. District Court for the Northern District of  
 6 California recently summarized how this process plays out:

7       To understand how the Meta Pixel typically works, imagine the following  
 8 scenario. A shoe company wishes to gather certain information on customers and  
 9 potential customers who visit its website. The shoe company first agrees to Meta’s  
 10 Business Tools Terms (discussed below), which govern the use of data from the  
 11 Pixel. The shoe company then customizes the Meta Pixel to track, say, every time  
 12 a site visitor clicks on the “sale” button on its website, which is called an “Event.”  
 13 Every time a user accesses the website and clicks on the “sale” button (i.e., an  
 14 “Event” occurs), it triggers the Meta Pixel, which then sends certain data to Meta.  
 15 Meta will attempt to match the customer data that it receives to Meta users—Meta  
 cannot match non-Meta users. The shoe company may then choose to create  
 16 “Custom Audiences” (i.e., all of the customers and potential customers who  
 17 clicked on the “sale” button) who will receive targeted ads on Facebook,  
 18 Instagram, and publishers within Meta’s Audience Network. Meta may also  
 19 provide the shoe company with de-identified, aggregated information so the shoe  
 20 company understands the impact of its ads by measuring what happens when  
 21 people see them. Meta does not reveal the identity of the matched Meta users to  
 22 the shoe company.

23       In re Meta Pixel Healthcare Litig., No. 22-CV-03580-WHO, 2022 WL 17869218, at \*2 (N.D.  
 24 Cal. Dec. 22, 2022) (internal citations omitted).<sup>32</sup>

25       67. Pixel also allows a company, like Defendant, to impact the delivery of ads,  
 26 measure cross-device conversions, create custom audiences, learn about its website, and save  
 27 money on advertising and marketing costs.<sup>33</sup> But, most relevant here, Pixel allowed Defendant  
 28 and Meta to track website users secretly on Defendant’s Website and intercept their  
 29 communications with Defendant. Indeed, Pixel is a bit of code that advertisers can integrate into  
 30

31  
 32 In describing Pixel technology in *In re Meta Pixel Healthcare Litig.*, the court referenced the declaration of expert  
 33 Richard M. Smith, which provides further details on the manner in which the challenged Pixel technology works  
 and Meta’s arrangements with health providers that employ it. 2022 WL 17869218, at \*2. See Declaration of  
 34 Richard M. Smith, filed in *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO (N.D. Cal.) [ECF 49].

35  
 36 <sup>33</sup>Meta Pixel, Facebook, [https://www.facebook.com/business/tools/meta-pixel?ref=search\\_new\\_2](https://www.facebook.com/business/tools/meta-pixel?ref=search_new_2) (last visited Sept.  
 37 14, 2023).

1      their website, mobile applications, and servers, thereby enabling Meta to intercept and collect  
 2 user activity on those platforms.

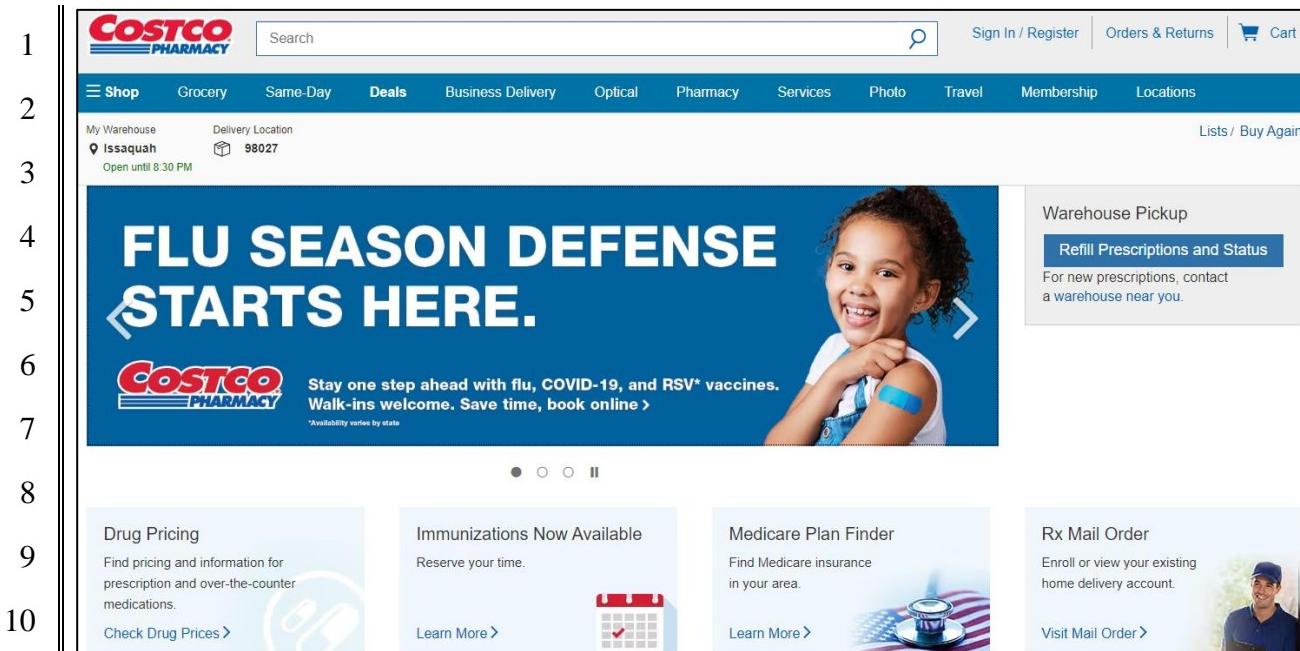
3        68. Thus, when visitors to Defendant's Website, like Plaintiffs and the Class  
 4 Members, communicated with Defendant or inquired about personal health-related topics, that  
 5 information was transmitted to Meta.

6        69. The Sensitive Information intercepted, recorded, and transmitted to Meta  
 7 includes, but is not limited to, computer IP addresses; patient status; prescription information  
 8 (including specific drugs and pricing information); immunization information; treatments;  
 9 patient location; and health insurance coverage. During that same transmission, Defendant  
 10 would also provide Meta with the patient's Facebook ID number, other persistent cookies, device  
 11 ID, or other PII. This information makes it easy to link private communications with Defendant  
 12 via the Website to a specific and identifiable Facebook user.

13       70. Once Meta has that data, it can process it, analyze it, and assimilate it into  
 14 databases like Core Audiences or Custom Audiences for advertising purposes. If the website  
 15 visitor is also a Facebook user, Meta will associate the information that it collects from the visitor  
 16 with a Facebook ID that identifies the user's name and Facebook profile. In sum, Pixel allows  
 17 Meta to learn, manipulate, and use for financial gain, the medical and private content Defendant's  
 18 Website visitors communicated, viewed, or otherwise interacted with on Defendant's Website.

### 19        **C. Defendant Deployed Pixel to Intercept and Record Sensitive Information**

20       71. As an example of how Pixel operates on Defendant's Website, consider a visitor  
 21 who opens Defendant's Website, and navigates to the Pharmacy webpage. When doing so, the  
 22 visitor's browser sends a GET Request to Defendant's server, requesting that server to load the  
 23 Pharmacy webpage, which is displayed below in *Figure 1*:



**Figure 1: Depiction of Pharmacy webpage**

72. At the same time, Pixel causes the visitor's browser to secretly intercept and record the visitor's communication with Defendant's Website, including the specific URL requested, and transmit the private communication to Meta along with unique identifiers used to link the communication to a specific Facebook user, as shown in **Figure 2**:

```

▼ Request Headers
:authority: www.facebook.com
:method: GET
:path: /tr?_
id=707542376568799&lev= PageView&dl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fware-
house-pickup&_l=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fwarehouse-
pickup&if=false&ts=1695150387059&sw=1920&sh=1080&v=2.9.127&r=stable&ec=0&o=308 fbp=
fb.1.1691010867087.1708375021|acs_est=true&it=1695150387016&coo=false&dpo=LDU&dpoco=0
&dpost=0&rqm=GET
:scheme: https
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Cookie: sb=UuDkZH5T8Pgney3DQbgBOZHW; datr=VeDkB6ZIJIG73XyPOIDfljS c_user=[REDACTED]
xs=28%3AV3U7Wbc3HTA-aA%3A2%3A1695142176%3A-1%3A-1;
fr=0pZwqaOjCx9fBASR.AWXo_9ws9rAJBIH9QdQHvOb-k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUlIp6lyEA
Pragma: no-cache
Referer: https://www.costco.com/

```

**Figure 2: Depiction of information intercepted and recorded by Meta.**

73. As reflected in **Figure 2**, the “path” shows the specific URL for the page requested by the visitor’s browser. It also shows the Pixel’s transmission of the \_fbp cookie, the c\_user cookie (the Facebook ID), and other cookies and identifiers used to identify the website visitor by name and Facebook account. Thus, the fact that a Costco Pharmacy patient or prospective patient is using or considering using the Costco Pharmacy is transmitted to Meta. Disclosure of that information reveals to Meta the website visitor’s status as a patient or prospective patient with Costco Pharmacy.

74. If that same visitor to the Costco Pharmacy webpage navigates to the “Drug Pricing” subpage, and enters the name of a prescription medication in the search bar, such as “Prozac,”<sup>34</sup> the visitor’s browser communicates a GET request to Defendant’s server to load the page shown below in ***Figure 3***:

Home / Member Prescription Program / Prozac

Brand/Generic  
Fluoxetine HCL (Generic)

Form  
Capsule

Strength  
20 mg

Package  
Bottle

Quantity  
90

# Prozac

Prices displayed are for **Fluoxetine HCL (Generic)**, Generic of Prozac (20 mg, 90 capsules)

**Pricing** Drug Information

Use your Costco membership number to save on prescription medications!



Find a participating pharmacy   Show membership card & prescription   Receive your Costco member price and save!

**COSTCO PHARMACY**

\$12.79

View Locations

*Figure 3: Depiction of search for “Prozac” pricing*

75. Because Defendant's Website uses Pixel, the visitor's private communications to Defendant's Website are also intercepted, recorded, and transmitted to Meta along with unique identifiers used to link the communications to a specific Facebook user, as shown in *Figure 4*:

<sup>34</sup> Prozac is a well-known antidepressant. Antidepressants, <https://my.clevelandclinic.org/health/treatments/9301-antidepressants-depression-medication> (last visited Sept. 19, 2023).

```
1  ▼ Request Headers
2   :authority: www.facebook.com
3   :method: GET
4   :path: /tr/
5   id=707542376568799&ev=Microdata&dl=https%3A%2F%2Fwww.costco.com%2Fcmpps%3FdrugIdentifierParam%3D55222865957
6   %26drugNameParam%3DProzac url=https%3A%2F%2Fwww.costco.com%2Fcmpp&if=false&ts=1695153451288&cd[DataLayer]=%
7   5B%5D&cd[Meta]=%7B%22title%22%3A%22%5Cn%20%20%20%5Ct%5Cn%20%20%20%5Ct%5CtProzac%20-
8   %20%5Cn%20%20%20%5CtMember%20Prescription%20Program%20Prices%5Cn%20%20%20%20%22%2C%22meta%3Adescription%22%3A%22Compare%20prices%20for%20Prozac%20and%20other%20drugs%20at%20your%20local%20pharmacies%20through%20Costco%2E%20%99s%20Membership%20Prescription%20Program.%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%7B%22dimensions%22%3A%7B%22h%22%3A20%2C%22w%22%3A1387%7D%2C%22properties%22%3A%7B%7D%2C%22subscopes%22%3A%5B%7B%22dimensions%22%3A%7B%22h%22%3A0%2C%22w%22%3A0%7D%2C%22properties%22%3A%7B%22item%22%3A%22%2F%22name%22%3A%22Home%22%2C%22position%22%3A%22%21%22%7D%2C%22subscopes%22%3A%5B%5D%2C%22type%22%3A%22https%3A%2F%2Fschema.org%2FListItem%22%7D%2C%7B%22dimensions%22%3A%7B%22%3A0%2C%22w%22%3A0%7D%2C%22properties%22%3A%7B%22item%22%3A%22%2Fcmpp%22%2C%22name%22%3A%22Member%20Prescription%20Program%22%2C%22position%22%3A%22%22%7D%2C%22subscopes%22%3A%5B%5D%2C%22type%22%3A%22https%3A%2F%2Fschema.org%2FListItem%22%7D%2C%7B%22dimensions%22%3A%7B%22h%22%3A0%2C%22w%22%3A0%7D%2C%22properties%22%3A%7B%22name%22%3A%22Prozac%22%2C%22position%22%3A%22%23%22%7D%2C%22subscopes%22%3A%5B%5D%2C%22type%22%3A%22https%3A%2F%2Fschema.org%2FBreadcrumbList%22%7D%5D&cd[JSON-LD]=%5B%5D&sw=1920&sh=1080&v=2.9.127&r=stable&ec=1&o=30&fb_=fb.1.1691010867087.17083750218&it=1695153450726&coo=false&dpo=LDU&dpoco=0&dpost=0&es=automatic&tm=3&rqm=Gt
9
10  :scheme: https
11  Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
12  Accept-Encoding: gzip, deflate, br
13  Accept-Language: en-US,en;q=0.9
14  Cache-Control: no-cache
15  Cookie: sb=UuDKZH5T8Pguey3DQbgBOZHW; datr=VeDkZB6ZIJIG73XyPOIDfJ5 c_user=[REDACTED] s=28%3AV3U7Wbc3HTA-aA%3A2%3A1695142176%3A-1%3A-1; fr=0pZwqaOjCjx9fBASR.AWXo_9ws9rAJBH9QdQHvOb-k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUlpxlyEAI
16  Pragma: no-cache
17  Referer: https://www.costco.com/
```

**Figure 4: Depiction of “Prozac” search intercepted and recorded by Meta.**

76. As another example, if a visitor to the Pharmacy webpage navigates to the “Immunizations Now Available,” subpage, the visitor can select from a variety of immunizations provided by Costco Pharmacy, including “Shingles (Shingrix),” resulting in the visitor’s browser transmitting a GET request to Defendant’s server to display the pages reflected below in ***Figures 5 and 6:***

1 Ask your pharmacist for details

2 Get Immunized at your local Costco Pharmacy Today!

3 Age restrictions may apply and vary by states. To save time, bring your completed and signed  
[immunization.consent.form](#).

4 You can also download the Costco Mobile app and search for Pharmacy. There you'll be able to  
fill out the immunization consent form and schedule your appointment straight from your smartphone.

5 How do I prepare for my immunization?

6 Immunizations and Vaccinations Available at your Costco Pharmacy

7 Prices listed is for one dose; some vaccinations require multiple doses to complete series  
Pricing reflects Costco Member Prescription Discount card which may vary by location and is subject to change. Revised 4/6/23

8 Seasonal Flu Vaccines for the Entire Family **starting at \$19.99** +

Hepatitis A (Havrix) **\$79.99** +

9 ***Figure 5: Depiction of “Immunizations Now Available” subpage.***

10 Pneumovax23® **\$118.99** +

11 Prevnar 20® **\$258.99** +

12 Shingles (Shingrix) **\$185.99** -

13 Shingles is a painful rash, often with blisters. Shingles is caused by the same virus that causes chickenpox; if you've had chickenpox, you can get shingles. Shingles is more common in adults over 50 years of age, and people with weakened immune systems. The shingles vaccine is recommended in adults 50 years of age and older.  
For more information about Shingles, [visit the Centers for Disease Control and Prevention website](#).  
[How do I prepare for my immunization?](#)

14 Possible side effects include:  
• Redness or soreness at the injection site  
• Headache  
• Allergic reaction (rare)

16 ***Figure 6: Depiction of “Shingles” selection.***

17 77. Because Defendant’s Website uses Pixel, the visitor’s private communications to  
18 Defendant about a specific vaccine—Shingles (Shingrix)—are also intercepted, recorded, and  
19 transmitted to Meta along with unique identifiers used to link the communications to a specific  
20 Facebook user, as shown in ***Figure 7***:

21

22

23

24

25

26

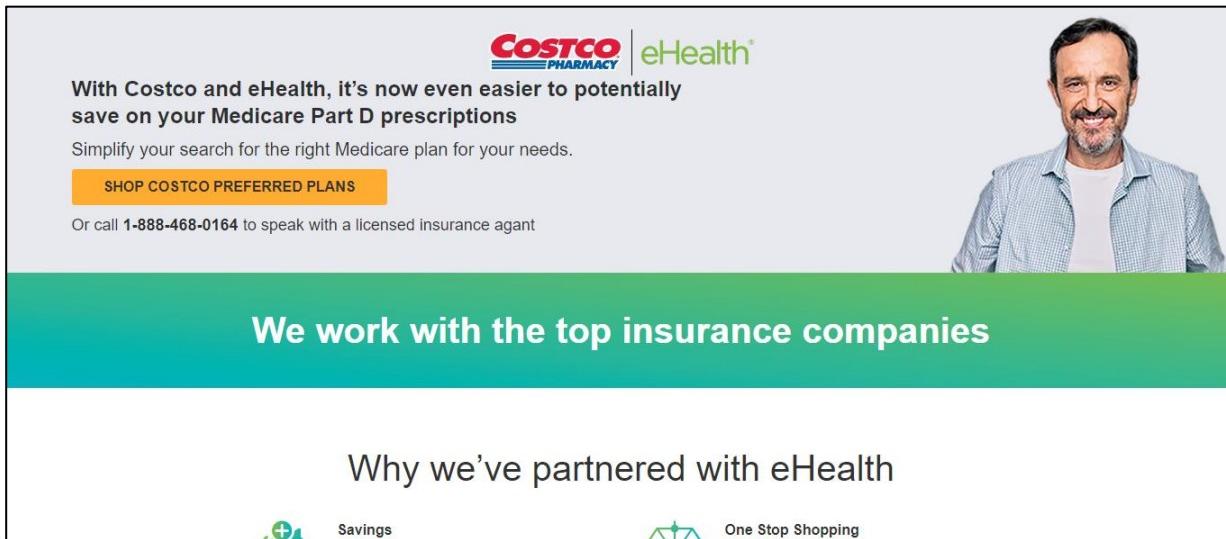
```

1   ▼ Request Headers
2     :authority: www.facebook.com
3     :method: GET
4     :path: /tr/?id=707542376568799&ev=SubscribedButtonClick&dl=https%3A%2Fwww.costco.com%2Fpharmacy%2Fadult-
5       immunization-program.html&rl=https%3A%2Fwww.costco.com%2Fpharmacy%2Fwarehouse-
6       pickup&it=false&ts=1695234029241&cd[buttonFeatures]=%7B%22classList%22%3A%22collapsed%22%2C%22destination%22-
7       %3A%22https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fadult-immunization-program.html%22%2C%22DrugName-
8       10%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22 Shingles%20(Shingrix) %22-
9       %C2%A0%20%C2%A0%20%24185.99%22%2C%22numChildButtons%22%3A%2C%22tag%22%3A%22a%22%2C%22type%22-
10      %3A%22null%22%2C%22name%22%3A%22%22%2D%2C%22buttonText%22%3A%22 Shingles%20(Shingrix) %20%2C%2A%0%20%2408%20%2C%22-
11      ormFeatures%22%5B%5D%2C%22pageFeatures%22%3A%22%22%2C%22Costco%20Pharmacy%20Immunization%20Program%20-
12      %7C%20Costco%22%7D%2C%22s=1920%2C%22sh=1080%2C%22v=2.9.127%2C%22r=stable%2C%22ec=2%2C%22o=10548%2C%22fbp%2C%22fb.1.1691010867087.1708375021%2C%22-
13      _est=true%2C%22it=1695234026297%2C%22coo=false%2C%22dpo=LDU%2C%22dpoco=0%2C%22post=0%2C%22es=automatic%2C%22tm=3%2C%22rqm=GEl%2C%22-
14      _user=%28%29%2C%22c_user=%28%29%2C%22s=28%2C%22AV3U7Wbc3HTA-
15      a%2C%22a%2C%221695142176%2C%22-1%2C%221%2C%22fr=0pZwqaOjCx9fBSR.AWXo_9ws9rAJ8IH9QdQHvOb-
16      k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUlIp6lyEAI%2C%22%2C%22no-cache%2C%22%2C%22Referer%2C%22https://www.costco.com/
17

```

**Figure 7: Depiction of “Shingles” search intercepted and recorded by Meta.**

78. Similarly, if a visitor then navigates to the “Medicare Plan Finder” subpage within the Pharmacy webpage, the visitor’s browser communicates a GET request to Defendant’s server to display the page shown in **Figure 8**, and that private communication is also intercepted and recorded by Meta along with the visitor’s unique identifiers as shown in **Figure 9**:



**Figure 8: Depiction of “Medicare Plan Finder” subpage.**

```

1   ▼ Request Headers
2     :authority: www.facebook.com
3     :method: GET
4     :path: /tr/
5       id=707542376568799&ev=Microdata&dl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fmedicare.l
6       tm
7       l&rI=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fwarehouse-
8       pickup&if=false&ts=1695158378248&cd[DataLayer]=%5B%5D&cd[Meta]=%7B%22title%22%3A%22Medicar
9       e%20%7C%20Costco%22%7D&cd[OpenGraph]=%7B%7D&cd[Schema.org]=%5B%5D&cd[JSON-
10      LD]=%5B%5D&sw=1920&sh=1080&v=2.9.127&r=stable&ec=1&o=30&fbp=fb.1.1691010867087.170837502
11      1&it=1695158376673&coo=false&dpo=LDU&dpoco=0&dpst=0&es=automatic&tm=3&rqm=GET
12      :scheme: https
13      Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*;q=0.8
14      Accept-Encoding: gzip, deflate, br
15      Accept-Language: en-US,en;q=0.9
16      Cache-Control: no-cache
17      Cookie: sb=UuDkZH5T8Pgney3DQbgBOZHW; datr=VeDkZB6ZIJIG73XyPOIDfljS_c_user=[REDACTED]
18      xs=28%3AV3U7Wbc3HTA-aA%3A2%3A1695142176%3A-1%3A-1;
19      fr=0pZwqaOjCjx9fBSR.AWXo_9ws9rAJBiH9QdQHvOb-k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUlpl6lyEAI
20      Pragma: no-cache
21      Referer: https://www.costco.com/

```

**Figure 9: Depiction of “Medicare Plan Finder” intercepted and recorded by Meta.**

79. By intercepting this information, Meta would know, for example, that a particular Facebook user was in the market for Medicare Part D prescription drug plans. And Meta would be able to monetize that private information by selling advertising to insurance companies seeking to market their Medicare Part D coverage to seniors.

80. As a final example, if a visitor to the Costco Pharmacy webpage navigates to the “Rx Mail Order” subpage, and clicks on “Refill Prescription,” the visitor’s browser sends a GET request to Defendant’s server, which displays a “Sign In” page as shown in **Figure 10**, and the visitor’s private communication about refilling a prescription is intercepted and recorded by Meta along with unique identifiers as shown in **Figure 11**:



Figure 10: Depicting “Rx Mail Order” subpage with “Refill Prescription” button

```

9    ▼ Request Headers
10   :authority: www.facebook.com
11   :method: GET
12   :path: /tr/?id=707542376568799&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fhome-
13   delivery&rl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fwarehouse-
14   pickup&if=false&ts=1695160443103&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20btn-primary%20btn-
15   block%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.costco.com%2FPharmacy%2Fhome-delivery-refill-
16   prescription%22%2C%22id%22%3A%22refill-prescription-
17   button%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Refill%20Prescriptions%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Refill%20Prescriptions&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22%5Cn%20%20%20%20%5CtWelcome%20to%20Costco%20Pharmacy%5Cn%20%20%20%20%22%7D&sw=1920&sh=1080&v=2.9.127&r=stable&ec=2&o=1054&fbp=fb.1.1691010867087.1708375021|xcs_est=true&it=1695160398189&coo=false&dpo=LDU&dpoco=0&dpst=0&es=automatic&xmt=3&rqm=GET
18   :scheme: https
19   Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
20   Accept-Encoding: gzip, deflate, br
21   Accept-Language: en-US,en;q=0.9
22   Cache-Control: no-cache
23   Cookie: sb=UuDkZH5T8Pguey3DQbg8OZHW; datr=VeDkZB6ZIJIG73XyPOIDfLj; c_user=[REDACTED]; s=28%3AV3U7Wbc3HTA-
24   aA%3A2%3A1695142176%3A-1%3A-1; fr=0pZwqaOjCjx9fBASR.AWvXo_9ws9raJB1H9QdQHvUb-
25   k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUlP6lyEAI
26   Pragma: no-cache
27   Referer: https://www.costco.com/

```

Figure 11: Depicting Meta’s interception and recording of communication regarding “Refill Prescription”

81. Based on the above examples of how Pixel operates on the Costco Pharmacy webpage, Meta would know (1) that a particular individual—who Meta could identify by name from the individual’s Facebook account—was a patient or prospective patient of the Costco Pharmacy seeking healthcare services, (3) that the named patient searched for pricing information for Prozac, a well-known antidepressant medication, (4) that the named patient inquired about the Shingles vaccine, (5) that the named patient was trying to refill prescriptions; and (6) that the

1 named patient was in the market for Medicare Part D prescription coverage. Meta would also  
 2 know the named patient's location and IP address, among other identifiers associated with the  
 3 patient's computer or cell phone. Using this Sensitive Information, Meta could put the named  
 4 patient into a Core or Custom Audience for purposes of targeted advertising by Costco or any  
 5 other company seeking to advertise its services or products to individuals that fit the named  
 6 patient's profile.

7       82. In this way, Meta, Costco, and other third parties profit off of Plaintiffs' and Class  
 8 Members' Sensitive Information without their knowledge, consent, or authorization.

9       83. Defendant deprived Plaintiffs and the Class Members of their privacy rights when  
 10 it: (a) embedded and implemented Pixel, which surreptitiously intercepted, recorded, and  
 11 disclosed Plaintiffs' and other online patients' and prospective patients' confidential  
 12 communications and private information; (b) disclosed patients' and prospective patients'  
 13 protected information to Meta—an unauthorized third party; and (c) failed to provide notice to  
 14 or obtain the consent from Plaintiffs and the Class Members to share their Sensitive Information  
 15 with others.

16           **D. Exposure of Sensitive Information Creates a Substantial Risk of Harm**

17       84. The Federal Trade Commission ("FTC") has recognized that consumer data is a  
 18 lucrative (and valuable) form of currency. In an FTC roundtable presentation, former  
 19 Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers  
 20 cannot begin to comprehend the types and amount of information collected by businesses, or why  
 21 their information may be commercially valuable. Data is currency."<sup>35</sup>

22       85. The FTC also issued, and regularly updates, guidelines for businesses to  
 23 implement reasonable data security practices and incorporate security into all areas of the  
 24 business. According to the FTC, reasonable data security protocols require, among other things:

---

25  
 26<sup>35</sup> Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable,  
 at 2 (Dec. 7, 2009) [https://www.ftc.gov/sites/default/files/documents/public\\_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf) (last visited Sept. 13, 2023).

1 (1) using industry tested and accepted methods; (2) monitoring activity on networks to uncover  
 2 unapproved activity; (3) verifying that privacy and security features function properly; and (4)  
 3 testing for common vulnerabilities or unauthorized disclosures.<sup>36</sup>

4       86. The FTC cautions businesses that failure to protect Sensitive Information and the  
 5 resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and  
 6 can take time, money, and patience to resolve the effect.<sup>37</sup> Indeed, the FTC treats the failure to  
 7 implement reasonable and adequate data security measures as an unfair act or practice prohibited  
 8 by Section 5(a) of the FTC Act.

9           **E. Plaintiffs' and the Class's Sensitive Information is Valuable**

10       87. As many health care data industry experts have recognized, "[p]atients' medical  
 11 data constitutes a cornerstone of the big data economy. A multi-billion dollar industry operates  
 12 by collecting, merging, analyzing[,] and packaging patient data and selling it to the highest  
 13 bidder."<sup>38</sup>

14       88. Thus, the personal, health, and financial information of Plaintiffs and the Class  
 15 Members is valuable and has become a highly desirable commodity. Indeed, one of the world's  
 16 most valuable resources is the exchange of personal data.<sup>39</sup>

17       89. Business News Daily reported that businesses collect personal data (i.e., gender,  
 18 web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction  
 19 with a business's website, applications, and emails), behavioral data (i.e., customers' purchase  
 20 histories and product usage information), and attitudinal data (i.e., consumer satisfaction data)

---

21  
 22       <sup>36</sup> *Start With Security, A Guide for Business*, FTC, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business> (last visited Sept. 13, 2023).

23       <sup>37</sup> See *Taking Charge: What to Do if Your Identity is Stolen*, FTC, at 2 (2012),  
<https://www.myoccur.org/sites/default/files/pdf/taking-charge-1.pdf> (last visited Sept. 13, 2023).

24       <sup>38</sup> Niam Yaraghi, *Who should profit from the sale of patient data?*, The Brookings Institution (Nov. 19, 2018),  
<https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/> (last visited Sept. 13, 2023).

25  
 26       <sup>39</sup> *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017),  
<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last visited Sept. 13, 2023).

1 from consumers.<sup>40</sup> Companies then use this data to impact the customer experiences, modify their  
 2 marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that  
 3 may be even more lucrative.<sup>41</sup>

4       90. The power to capture and use customer data to manipulate products, solutions,  
 5 and the buying experience is invaluable to a business's success. Research shows that  
 6 organizations who "leverage customer behavioral insights outperform peers by 85 percent in  
 7 sales growth and more than 25 percent in gross margin."<sup>42</sup>

8       91. In 2013, the Organization for Economic Cooperation and Development  
 9 ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of  
 10 Methodologies for Measuring Monetary Value."<sup>43</sup> In this paper, the OECD measured prices  
 11 demanded by companies concerning user data derived from "various online data warehouses."<sup>44</sup>

12       92. OECD indicated that "[a]t the time of writing, the following elements of personal  
 13 data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., \$2] for a date  
 14 of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's  
 15 license number and USD 35 for a military record. A combination of address, date of birth, social  
 16 security number, credit record and military is estimated to cost USD 55."<sup>45</sup>

17       93. Unlike financial information, such as credit card and bank account numbers, the  
 18 PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are  
 19  
 20

---

21  
 22 <sup>40</sup> Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY  
 23 (Aug. 5, 2022; updated May 30, 2023), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>  
 24 (last visited Sept. 13, 2023).

25       <sup>41</sup> *Id.*

26       <sup>42</sup> Brad Brown, et al. *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017),  
 27 <https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data>  
 28 (last visited Sept. 13, 2023).

29       <sup>43</sup> Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD  
 30 Digital Economy Papers, No. 220, OECD PUBLISHING PARIS (Apr. 2, 2013),  
 31 <https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf> (last visited Sept. 13, 2023).

32       <sup>44</sup> *Id.* at 25.

33       <sup>45</sup> *Id.*

1 given at birth and attach to a person for the duration of his or her life. Medical histories are  
 2 inflexible. For these reasons, these types of information are the most lucrative and valuable.<sup>46</sup>

3       94. Consumers place considerable value on their Sensitive Information and the  
 4 privacy of that information. One 2002 study determined that U.S. consumers highly value a  
 5 website's protection against improper access to their Sensitive Information, between \$11.33 and  
 6 \$16.58 per website. The study further concluded that to U.S. consumers, the collective  
 7 "protection against errors, improper access, and secondary use of personal information is worth  
 8 between US\$30.49 and \$44.62.<sup>47</sup> This data is approximately twenty years old, and the dollar  
 9 amounts would likely be exponentially higher today.

10       95. Defendant's privacy violations exposed a variety of Sensitive Information,  
 11 including patient status, prescription information, immunization information, health insurance  
 12 coverage, and other highly sensitive data.

13       96. PHI, like that exposed here, is likely even more valuable than Social Security  
 14 numbers and just as capable of being misused.<sup>48</sup> PHI can be ten times more valuable than credit  
 15 card information.<sup>49</sup> This is because one's personal health history, including prior illness,  
 16 surgeries, diagnoses, mental health, prescriptions, and the like cannot be changed or replaced,  
 17 unlike credit card information and even, under difficult circumstances, Social Security  
 18 numbers.<sup>50</sup>

---

19  
 20       <sup>46</sup> *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy  
 Enters (July 21, 2020), <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/> (last visited Sept. 13, 2023).

21       <sup>47</sup> Il-Horn Hann, Kai-Lung Hui *et al.*, *The Value of Online Information Privacy: Evidence from the USA and Singapore*, at 17, Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), <https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited Sept. 13, 2023).

22       <sup>48</sup> *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), [https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=\(U\)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market](https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=(U)%20Cyber%20actors%20will%20likely,records%20in%20the%20black%20market). (last visited Sept. 13, 2023).

23       <sup>49</sup> Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Sept. 13, 2023).

24       <sup>50</sup>*Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sept. 13, 2023). Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she

1       97. Indeed, prescription records, blood tests, doctor notes, hospital visits, and  
 2 insurance records are all sold to commercial companies, which gather years of health information  
 3 on hundreds of millions of people and then sell it to other industries, like pharmaceutical  
 4 companies who use the information to sell more drugs.<sup>51</sup> Some industry insiders and journalists  
 5 are even calling hospitals the “brokers to technology companies” for their role in data sharing in  
 6 the \$3 trillion healthcare sector.<sup>52</sup> “Rapid digitization of health records . . . have positioned  
 7 hospitals as a primary arbiter of how much sensitive data is shared.”<sup>53</sup>

8           **F. Plaintiffs and the Class Had a Reasonable Expectation of Privacy in Their  
 9 Interaction with Defendant’s Website**

10       98. Consumers are concerned about companies, like Defendant, collecting their data  
 11 and assume the data they provide, particularly highly sensitive medical and insurance data, will  
 12 be kept secure and private.

13       99. In a recent survey related to Internet user expectations, most website visitors  
 14 indicated that their detailed interactions with a website should only be used by the website and  
 15 not be shared with a party they know nothing about.<sup>54</sup> Thus, website visitors reasonably expect  
 16 that their interactions with a website should not be released to third parties unless explicitly  
 17 stated.<sup>55</sup>

18

---

19 continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and  
 20 will continue in the future. The Social Security Administration warns that the unauthorized disclosure of a Social  
 21 Security number can lead to identity theft and fraud. Social Security Administration, *Identity Theft and Your Social  
 Security Number*, at 1, 56, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Sept. 13, 2023).

22       <sup>51</sup> Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Industry*, TIME (Jan. 9, 2017),  
<https://time.com/4588104/medical-data-industry/> (last visited Sept. 13, 2023)

23       <sup>52</sup> Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, The Wall Street Journal (Jan.  
 20, 2020), <https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200> (last visited Sept. 13, 2023).

24       <sup>53</sup> *Id.*

25       <sup>54</sup> See *Privacy and Online Tracking Perceptions Survey Report* (March 2020), CUJOAI, at 15–19, Privacy  
 Survey\_03-24 ([cujo.com](http://cujo.com)) (indicating major concerns of survey respondents was illegal use of data and unethical  
 tracking and indicating respondents’ belief that responsibility allocation falls on websites, and Internet users should  
 be able to turn to the websites themselves, for privacy breaches).

26       <sup>55</sup> Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE  
 INFORMATION SOCIETY, 38:4, 257, 258 (2022).

1       100. The majority of Americans consider one of the most important privacy rights to  
 2 be the need for an individual's affirmative consent before a company collects and shares its'  
 3 customers' data.<sup>56</sup> A March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents  
 4 were uncomfortable with web tracking schemes where data was combined with an individual's  
 5 identity.<sup>57</sup> The same poll found that 63 percent of respondents were uncomfortable with web  
 6 tracking even where the clickstream data was not linked to personally identifiable information.<sup>58</sup>  
 7 A July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking  
 8 computer use was an invasion of privacy.<sup>59</sup>

9       101. Patients and website users act consistently with their expectation of privacy. For  
 10 example, following a new rollout of the iPhone operating software—which asks users for clear,  
 11 affirmative consent before allowing companies to track users—85 percent of worldwide users  
 12 and 94 percent of U.S. users chose not to allow such tracking.<sup>60</sup>

13       102. Like the greater population, Defendant's patients and prospective patients would  
 14 expect the highly sensitive medical information they provided to Defendant through the Website  
 15 to be kept secure and private.

16       **G. Defendant's Conduct Violates HIPAA**

17       103. Under HIPAA, individuals' health information must be:

18       properly protected while allowing the flow of health information needed to provide  
 19 and promote high quality health care and to protect the public's health and well-  
 20 being. The [Privacy] Rule strikes a balance that permits important uses of  
 21 information, while protecting the privacy of people who seek care and healing.<sup>61</sup>

---

22  
 23       <sup>56</sup> *Public Opinion on Privacy*, EPIC.ORG, <https://archive.epic.org/privacy/survey/>.

24       <sup>57</sup> *Id.*

25       <sup>58</sup> *Id.*

26       <sup>59</sup> *Id.*

27       <sup>60</sup> Margaret Taylor, *How Apple screwed Facebook*, WIRED (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

28       <sup>61</sup> U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (Oct. 19, 2022),  
 29 <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 27, 2023).

1       104. HIPAA “is a federal law that required the creation of national standards to  
 2 protect sensitive patient health information from being disclosed without the patient’s  
 3 consent or knowledge.”<sup>62</sup> The rule requires appropriate administrative, physical, and  
 4 technical safeguards to ensure the confidentiality, integrity, and security of electronic  
 5 protected health information.<sup>63</sup>

6       105. HIPAA defines “protected health information” as “individually identifiable health  
 7 information” that is “created or received by a health care provider” (or similar entities) that  
 8 “[r]elates to past, present, or future physical or mental health or condition of an individual; the  
 9 provision of health care to an individual; or the past, present, or future payment for the provision  
 10 of health care to an individual.” 45 C.F.R. § 160.103. Identifiers such as patient-status (i.e.,  
 11 information that connects a particular user to a particular health care provider), medical  
 12 conditions, prescription information, or health insurance coverage and payment, gathered in this  
 13 case by Pixel through Costco’s Website, constitute protected health information.

14       106. Additionally, HIPAA defines sensitive patient personal and health information as:  
 15 (1) name; (2) home and work addresses; (3) home and work phone numbers; (4) personal and  
 16 professional email addresses; (5) medical records; (6) prescriptions; (7) health insurance  
 17 information; (8) billing information; (9) Social Security number; (10) spouse and children’s  
 18 information; and/or (11) emergency contact information.<sup>64</sup>

19       107. To ensure protection of this private and sensitive information, HIPAA mandates  
 20 standards for handling PHI—the very data Defendant failed to protect. The privacy violations  
 21 described herein resulted from Defendant’s failure to comply with several of these standards:

---

22       <sup>62</sup> *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, Centers for Disease Control and Prevention  
 23 (June 27, 2022), [https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20\(HIPAA\),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge](https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge) (last visited Aug. 19, 2022).

24  
 25       <sup>63</sup> U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (Oct. 19, 2022),  
<https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 28, 2023).

26       <sup>64</sup> See *What is Considered Protected Health Information Under HIPAA*, HIPAA Journal (Jan. 2, 2022); U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 28, 2023).

- 1           a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and  
2                 integrity of electronic protected health information that Defendant creates,  
3                 receives, maintains, and transmits;
- 4           b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies  
5                 and procedures for electronic information systems that maintain electronic  
6                 protected health information to allow access only to those persons or software  
7                 programs that have been granted access rights;
- 8           c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and  
9                 procedures to prevent, detect, contain, and correct security violations;
- 10          d. Violation of 45 C.F.R. § 164.306(a)(2): Failing to protect against any reasonably  
11                 anticipated threats or hazards to the security or integrity of electronic protected  
12                 health information;
- 13          e. Violation of 45 C.F.R. § 164.306(a)(3): Failing to protect against any reasonably  
14                 anticipated uses or disclosures of electronical protected health information that  
15                 are not permitted or required under the privacy rules regarding individually  
16                 identifiable health information;
- 17          f. Violation of 45 C.F.R. § 164.306(a)(4): Failing to ensure compliance with HIPAA  
18                 security standard rules by its workforce;
- 19          g. Violation of 45 C.F.R. § 164.502 et seq.: Impermissibly and improperly using and  
20                 disclosing protected health information that is, and remains, accessible to  
21                 unauthorized persons; and
- 22          h. Violation of 45 C.F.R. § 164.530(c): Failing to design, implement, and enforce  
23                 policies and procedures establishing administrative, technical, and physical  
24                 safeguards to reasonably protect the privacy of protected health information.

25          108. Additionally, according to the U.S. Department of Health and Human Services'

26          Health Information Privacy Bulletin ("HHS Privacy Bulletin"), HIPAA covered entities cannot

1 share PHI or PII to online tracking technology vendors for marketing purposes without first  
 2 obtaining the individual's HIPAA-compliant authorization.<sup>65</sup> The HHS Privacy Bulletin  
 3 explicitly states:

4       The HIPAA Rules apply when the information that regulated entities collect through  
 5 tracking technologies or disclose to tracking technology vendors includes protected  
 6 health information (PHI). Some regulated entities may share sensitive information with  
 7 online tracking technology vendors and such sharing may be unauthorized disclosures of  
 8 PHI with such vendors. **Regulated entities are not permitted to use tracking**  
**technologies in a manner that would result in impermissible disclosures of PHI to**  
**tracking technology vendors or any other violations of the HIPAA Rules.** For  
 9 example, disclosures of PHI to tracking technology vendors for marketing purposes,  
 10 without individuals' HIPAA-compliant authorizations, would constitute impermissible  
 11 disclosures.<sup>66</sup>

109. The HHS Privacy Bulletin also identifies several harms that may result from an  
 11 impermissible disclosure of an individual's PHI, including:

12       identity theft, financial loss, discrimination, stigma, mental anguish, or other serious  
 13 negative consequences to the reputation, health, or physical safety of the individual or to  
 14 others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive  
 15 information about an individual, including diagnoses, frequency of visits to a therapist or  
 16 other health care professionals, and where an individual seeks medical treatment. While  
 17 it has always been true that regulated entities may not impermissibly disclose PHI to  
 18 tracking technology vendors, because of the proliferation of tracking technologies  
 19 collecting sensitive information, now more than ever, it is critical for regulated entities to  
 20 ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA  
 21 Privacy Rule.<sup>67</sup>

110. According to HHS, HIPAA "[r]egulated entities disclose a variety of information  
 12 to tracking technology vendors through tracking technologies placed on a regulated entity's  
 13 website or mobile app, including individually identifiable health information [] that the individual  
 14 provides when they use regulated entities' websites or mobile apps."<sup>68</sup> The information an  
 15 individual provides may include a "medical record number, home or email address, or dates of  
 16

---

24       <sup>65</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH  
 25 AND HUMAN SERVICES (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

26       <sup>66</sup> *Id.* (internal citations omitted) (emphasis in original).

<sup>67</sup> *Id.* (internal citations omitted) (emphasis in original).

<sup>68</sup> *Id.*

1 appointments, as well as an individual's IP address or geographic location, medical device IDs,  
2 or any unique identifying code.”<sup>69</sup>

3        111. All of the above listed information that is collected on a regulated entity's website,  
4 like Defendant's Website, is PHI, "even if the individual does not have an existing relationship  
5 with the regulated entity and even if the [information], such as IP address or geographic location,  
6 does not include specific treatment or billing information like dates and types of health care  
7 services."<sup>70</sup> When a regulated entity, again like Defendant, collects the individual's information,  
8 that information connects the individual to the regulated entity (i.e., it is indicative that the  
9 individual has received or will receive health care services or benefits from the covered entity),  
10 and thus relates to the individual's past, present, or future health or health care or payment for  
11 care.<sup>71</sup>

12        112. As a health care provider, delivering “services . . . related to the health of an  
13 individual,” including the “[s]ale or dispensing of a drug . . . in accordance with a prescription,”  
14 Defendant is a “covered entity” and therefore subject to the requirements under HIPAA.<sup>72</sup> See  
15 45 C.F.R. § 160.103 (defining “covered entity,” “health care provider,” and “health care”). Yet,  
16 by embedding and deploying Pixel, Defendant blatantly disregarded these rules, placing profit  
17 over patient privacy and confidentiality, and therein violated the rights of its patients and  
18 prospective patients.

CLASS PERIOD

20        113. For purposes of this Class Action Complaint, the Class Period corresponds to the  
21 period between October 2020 and the present and runs until such date as the Court enters an  
22 Order certifying any Count of this Class Action Complaint for class action treatment.

25 | 69 *Id.*

70 *Id.*

26 | 71 - 1

<sup>72</sup> Defendant acknowledges as much given its Notice of Privacy Practices. See *supra*.

## **CLASS ACTION ALLEGATIONS**

114. Plaintiffs bring this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and all others similar situated, as representatives of the following Class:

All individuals residing in the United States whose Sensitive Information was disclosed to a third party through Defendant’s Website without authorization or consent during the Class Period.

115. Excluded from the Class is Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

116. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating subclasses, as necessary.

117. All members of the proposed Class are readily identifiable through Defendant's records.

118. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and  
23(b)(3) are satisfied.

**119. Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class includes at least one million people. The precise number of the Class Members is unknown to the Plaintiffs but may be ascertained from Defendant's records.

120. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiffs and the Class Members, which predominate over any questions only affecting individual Class Members. These common legal and factual questions include, without limitation:

- 1           a. Whether Plaintiffs' and Class Members' private communications were  
2           intercepted and recorded;
- 3           b. Whether the interception and recording of Plaintiffs' and Class Members'  
4           communications was consensual;
- 5           c. Whether Defendant owed Plaintiffs and the other Class Members a duty to  
6           adequately protect their Sensitive Information;
- 7           d. Whether Defendant owed Plaintiffs and the other Class Members a duty to secure  
8           their Sensitive Information from disclosure via third-party tracking technologies;
- 9           e. Whether Defendant owed Plaintiffs and the other Class Members a duty to  
10          implement reasonable data privacy protection measures because Defendant  
11          accepted, stored, created, and maintained highly sensitive information concerning  
12          Plaintiffs and the Class;
- 13          f. Whether Defendant knew or should have known of the risk of disclosure of data  
14          through third-party tracking technologies;
- 15          g. Whether Defendant breached its duty to protect the Sensitive Information of  
16          Plaintiffs and the other Class Members;
- 17          h. Whether Defendant knew or should have known about the inadequacies of its  
18          privacy protection;
- 19          i. Whether Defendant failed to use reasonable care and reasonable methods to  
20          safeguard and protect Plaintiffs' and the Class's Sensitive Information from  
21          unauthorized disclosure;
- 22          j. Whether proper data security measures, policies, procedures, and protocols were  
23          enacted within Defendant's computer systems to safeguard and protect Plaintiffs'  
24          and the Class's Sensitive Information from unauthorized disclosure;
- 25          k. Whether Defendant's conduct was the proximate cause of Plaintiffs' and the  
26          Class's injuries;

- 1       1. Whether Plaintiffs and the Class Members had a reasonable expectation of privacy  
2            in their Sensitive Information;
- 3       m. Whether Plaintiffs and the Class Members suffered ascertainable and cognizable  
4            injuries as a result of Defendant's misconduct;
- 5       n. Whether Plaintiffs and the Class Members are entitled to recover damages; and
- 6       o. Whether Plaintiffs and the Class Members are entitled to other appropriate  
7            remedies including injunctive relief.

8       121. Defendant engaged in a common course of conduct giving rise to the claims  
9 asserted by Plaintiffs on behalf of themselves and the Class. Individual questions, if any, are  
10 slight by comparison in both quality and quantity to the common questions that control this  
11 action.

12       122. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because  
13 Plaintiffs' Sensitive Information, like that of every other Class Member, was improperly  
14 disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar  
15 manner.

16       123. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests  
17 of the members of the Class and have retained counsel experienced in complex consumer class  
18 action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or  
19 antagonistic interests to those of the Class.

20       124. **Superiority.** A class action is superior to all other available methods for the fair  
21 and efficient adjudication of this controversy. The damages or other financial detriment suffered  
22 by individual Class Members are relatively small compared to the burden and expense that would  
23 be entailed by individual litigation of their claims against Defendant. The adjudication of this  
24 controversy through a class action will avoid the possibility of inconsistent and potentially  
25 conflicting adjudications of the asserted claims. There will be no difficulty in managing this  
26 action as a class action, and the disposition of the claims of the Class Members in a single action

will provide substantial benefits to all parties and to the Court. Absent a class action, individual patients like Plaintiffs would find the cost of litigating their claims prohibitively high and would have no effective remedy for monetary relief.

125. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant has acted or refused to act on grounds that apply generally to the Class, thereby making monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As Defendant continues to engage in the practices described herein, the risk of future harm to Plaintiffs and the Class remains, making injunctive relief appropriate. The prosecution of separate actions by all affected individuals with injuries similar to Plaintiffs', even if possible, would create a substantial risk of (a) inconsistent or varying adjudications with respect to individual patients, which would establish potentially incompatible standards of conduct for Defendant, and/or (b) adjudications with respect to individual patients which would, as a practical matter, be dispositive of the interests of the other patients not parties to the adjudications, or which would substantially impair or impede the ability to protect the interests of the Class. Further, the claims of individual patients in the defined Class are not sufficiently large to warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

## LEGAL CLAIMS

**COUNT I**

## **Violation of the Electronic Communications Privacy Act (“ECPA”)**

**18 U.S.C. § 2511(1)**

**(By Plaintiffs and on behalf of the Nationwide Class)**

126. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

127. The Electronic Communications Privacy Act (“ECPA”) protects against the intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

<sup>128</sup> The ECPA further provides any person who

1                             (c) intentionally discloses, or endeavors to disclose, to any other person the contents of  
 2 any wire, oral, or electronic communication, knowing or having reason to know that the  
 3 information was obtained through the interception of a wire, oral, or electronic  
 4 communication in violation of this subsection;

5                             (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic  
 6 communication, knowing or having reason to know that the information was obtained  
 7 through the interception of a wire, oral, or electronic communication in violation of this  
 8 subsection.

9                             Shall be punished as provided in subsection (4) or shall be subject to suit as provided in  
 10 subsection (5).

11                         *Id.* §§ 2511(1)(c) & (d).

12                         129. The primary purpose of the ECPA is to protect the privacy and security of  
 13 communications as technology evolves.

14                         130. Section 2511 of the ECPA provides that, for violations of the Act, the Court “may  
 15 use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and  
 16 shall impose a civil fine of not less than \$500 for each violation of such an injunction.” *Id.* §  
 17 2511(5)(b).

18                         131. Section 2520 provides a private right of action to any person whose wire or  
 19 electronic communications are intercepted, disclosed, or intentionally used. Specifically, Section  
 20 2520 states that “any person whose wire, oral, or electronic communication is intercepted,  
 21 disclosed, or intentionally used in violation of [Chapter 119] may in a civil action recover from  
 22 the person or entity . . . , which engaged in that violation” in a civil action. *Id.* § 2520(a).

23                         132. The ECPA defines “intercept[ion]” as the “acquisition of the contents of any wire,  
 24 electronic, or oral communication through the use of any electronic, mechanical, or other device.”  
 25 *Id.* § 2510(4).

26                         133. The ECPA defines “contents,” when used with respect to electronic  
 27 communications, to “include[] any information concerning the substance, purport, or meaning of  
 28 that communication.” *Id.* § 2510(8).

29                         134. “Electronic communication” means “any transfer of signs, signals, writing,  
 30 images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,

1 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign  
 2 commerce.” *Id.* § 2510(12).

3       135. “Electronic, mechanical or other device” means “any device or apparatus which  
 4 can be used to intercept . . . electronic communication[s].” *Id.* § 2510(5). Here, Plaintiffs’ and  
 5 the Class Members’ browsers and computing devices and Defendant’s webservers, Website, and  
 6 Pixel code Defendant deployed are all “devices” for the purposes of the ECPA.

7       136. The transmissions of Plaintiffs’ and the Class Members’ Sensitive Information to  
 8 Defendant’s Website violates the ECPA. The transmissions from Plaintiffs and the Class  
 9 Members to Defendant, through Defendant’s Website ([www.costco.com](http://www.costco.com)) are “electronic  
 10 communications” under the ECPA. *See id.* § 2510(12).

11       137. Indeed, Defendant’s use of Pixel unlawfully and intentionally disclosed Plaintiffs’  
 12 and the Class Members’ Sensitive Information to Meta, including but not limited to, information  
 13 regarding patient status, past and current prescription medications, treatments and care options,  
 14 immunizations, location, medication research, health insurance coverage, and other sensitive  
 15 information. These intentional acts violate several sections of the ECPA. *See id.* §§ 2511(1)(a),  
 16 (c)–(d).

17       138. By embedding and deploying Pixel on Defendant’s Website, Defendant  
 18 intentionally violated the ECPA, through its interception, attempt at interception, and its  
 19 procurement of Meta to intercept the electronic communications of Plaintiffs and the Class  
 20 Members. Defendant also intentionally used or attempted to use the contents of Plaintiffs’ and  
 21 the Class Members’ electronic communications, knowing that the information was obtained  
 22 through interception. Defendant’s use of confidential and private patient information and data  
 23 for advertising and other revenue generating benefits, in the absence of express written consent,  
 24 violated ECPA.

25

26

1       139. Further, by embedding Pixel on its Website and disclosing the content of patient  
 2 communications relating to Sensitive Information, without consent, Defendant had a purpose that  
 3 was tortious, criminal, and designed to violate state and federal laws including:

- 4           a. An invasion of privacy;
- 5           b. A violation of the Washington Uniform Health Care Information Act;
- 6           c. A violation of the Washington Consumer Protection Act;
- 7           d. A violation of the Washington cybercrime act (RCW 9A.90);
- 8           e. A violation of 42 U.S.C. § 1320d–6, the Administrative Simplification subtitle  
             of HIPAA, which protects against the disclosure of individually identifiable  
             health information to another person and is a criminal offense punishable by  
             fine or imprisonment; and
- 12          f. A violation of HIPAA.

13       140. Additionally, Defendant had no legitimate purpose for intentionally intercepting  
 14 the contents of Plaintiffs' and the Class Members' private and personal electronic  
 15 communications. And even if Defendant could identify *some* legitimate purpose, it would not  
 16 outweigh the egregious breach and invasion of privacy Defendant has committed against  
 17 Plaintiffs and the Class Members.

18       141. At no time did Plaintiffs and the Class Members provide their consent to  
 19 Defendant's disclosure of their Sensitive Information to Meta and/or other third parties.

20       142. Further, Defendant has improperly profited from its invasion of Plaintiffs' and the  
 21 Class Members' privacy in its use of their data for its economic value.

22       143. Defendant knew that such conduct would be highly offensive. Regardless, it  
 23 proceeded to embed Pixel and use it to the detriment of visitors to its Website.

24       144. Plaintiffs and the Class Members are entitled to damages, including statutory,  
 25 compensatory and/or nominal damages in an amount to be proven at trial.

145. Defendant's conduct is ongoing, and it continues to unlawfully disclose and use the intercepted communications of Plaintiffs and the Class Members any time they provide information to Defendant through its Website without their consent. Plaintiffs and the Class Members are therefore entitled to declaratory and injunctive relief. Such relief will prevent future unlawful and unauthorized disclosure of Plaintiffs' and the Class Members' Sensitive Information.

## COUNT II

## **Violation of the Washington Privacy Act**

**Wash. Rev. Code § 9.73.030 et seq.**

**(By Plaintiffs and on behalf of the Nationwide Class)**

146. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

147. The Washington Privacy Act (the “Act”) makes it unlawful for “any individual, partnership, corporation, [or] association . . . to intercept[] or record” any “[p]rivate communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication.”

Wash. Rev. Code § 9.73.030(1)(a).

148. The Act further states that “[a]ny person who, directly or by means of a detective agency or any other agent, violates the provisions of [Chapter 9.73] shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of [Chapter 9.73], or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney’s fee and other costs of litigation.” *Id.* § 9.73.060.

1       149. Costco is a person for purposes of the Act because it is a corporation. *Id.* §§  
 2 9.73.030(1), 9.73.060.

3       150. Plaintiffs' and the Class Members' intercepted and recorded Website  
 4 Communications related to their Sensitive Information constitute "private communications"  
 5 within the meaning of the Act. *See id.*

6       151. Plaintiffs' and the Class Members' electronic devices and web browsers, and  
 7 Defendant's webserver and Website are "devices" through which the private communications  
 8 were transmitted between points within or without the state of Washington.

9       152. Online tracking technology like Pixel, provided by Meta and procured by  
 10 Defendant, is a "device" that is "designed to record and/or transmit [private] communications"  
 11 within the meaning of the Act. *See id.* § 9.73.030(1)(a).

12       153. Defendant intentionally procured and embedded third-party tracking technology,  
 13 Pixel, on its Website, including on its Pharmacy webpage, to secretly intercept and record  
 14 Plaintiffs' and the Class Members' private communications with Costco in real time, including  
 15 communications regarding prescriptions and immunizations, among other Sensitive Information.  
 16 Defendant violated the Act directly and by means of an agent—Meta—by intercepting and  
 17 recording Plaintiffs' and Class Members' private communications with Defendant via the Meta  
 18 Pixel.

19       154. Defendant did so for its own profit and gain, disclosing its patients' and  
 20 prospective patients' sensitive health information to third parties, like Meta, in an effort to drive  
 21 visits to its website using more sophisticated and targeted advertising based on data harvested  
 22 from its website visitors.

23       155. As participants in the communications, Plaintiffs and the Class Members did not  
 24 consent to having their Website Communications secretly intercepted and recorded.

25       156. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class  
 26 Members were injured in their "person[s]," RCW 9.73.060, including through interference with

their control over their personal data, intrusion into their private affairs, the highly offensive publication of private facts, and other losses of privacy related to the secret interception and disclosure of their private and sensitive health information.

157. Under Section 9.73.060, Plaintiffs and the Class Members seek (1) actual damages, not less than liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and (2) reasonable attorneys' fees and other costs of litigation incurred. Wash. Rev. Code § 9.73.060.

**COUNT III**

**Violation of the Washington Consumer Protection Act (“WCPA”)  
Wash. Rev. Code § 19.86 et seq.**

**(By Plaintiffs and on behalf of the Nationwide Class)**

158. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

159. The Washington Consumer Protection Act (“WCPA”), Washington Revised Code Section 19.86 et seq., prohibits “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Wash. Rev. Code § 19.86.020.

160. The elements of a WCPA claim are (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) impacting the public interest, (4) an injury to plaintiff in her business or property, and (5) a causal relationship between the unfair or deceptive act and the resulting injury. *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 719 P.2d 531, 535–40 (Wash. 1986).

161. Defendant engaged in unfair or deceptive acts, omissions, and practices in the conduct of trade or commerce, in violation of Section 19.86.020, by violating Plaintiffs' and the Class Members' rights to privacy and by embedding and implementing tracking technologies, like Pixel, on its Website, to secretly record and disclose Plaintiffs' and the Class Members' private communications, including their highly sensitive health information, without their consent.

1       162. Defendant shared its collected data with third parties, like Meta, for profit or other  
 2 business purposes, which further violates the WCPA and is an unfair or deceptive act or practice.

3       163. Defendant committed its conduct in the context of trade or commerce. Costco  
 4 offers pharmaceutical services and other health-related services in interstate commerce in  
 5 markets across the nation. In addition, visitors to Costco's Website can use the Website to  
 6 purchase prescriptions, immunizations, and conduct other health-related activities. Costco uses  
 7 its covert recordings of patients' and prospective patients' Website Communications, including  
 8 Sensitive Information, for business purposes affecting interstate commerce, including by  
 9 providing patient and prospective patient personal and health-related data to third parties, like  
 10 Meta, for profit.

11       164. The public interest is harmed by Defendant's conduct in embedding and  
 12 implementing tracking technologies, like Pixel, on its Website to intercept, record, and disclose  
 13 millions of Americans' private and protected communications, including their highly personal  
 14 information, to unauthorized third parties. This includes Plaintiffs and the Class Members who  
 15 have a fundamental privacy interest in that information. Indeed, Costco's unlawful procurement  
 16 of individuals' personal and health-related data, some of the most sensitive nature, without their  
 17 consent has large ramifications on the privacy interest of those individuals. In addition, to the  
 18 extent that Costco uses this information for improvements to its services or transmits such  
 19 information to third parties for profit or another benefit, Costco is deriving an unfair competitive  
 20 advantage because of its covert recording and unauthorized disclosures.

21       165. By embedding Pixel on its Website and disclosing, without consent, the content  
 22 of patient and prospective patient communications relating to prescriptions and immunizations,  
 23 among other Sensitive Information, Plaintiffs and the Class Members have been harmed in their  
 24 privacy interests. Furthermore, Defendant's actions have and continue to injure Plaintiffs and the  
 25 Class Members because their private communications, including their highly sensitive health

1 information, is being used, and continues to be used, for commercial gain—all without their  
 2 knowledge or consent.

3       166. Plaintiffs and the Class Members expected their communications would remain  
 4 private such that they could freely interact with Defendant's Website and disclose private,  
 5 personal information for the purpose of receiving health care services or health care-related  
 6 information and knowledge. At no time did Plaintiffs and the Class Members ever expect that  
 7 Costco would unlawfully and surreptitiously share their private and protected communications,  
 8 including their highly personal health information, to third parties by using the embedded third-  
 9 party tracking technology, Pixel, on Defendant's Website. Such considerations are material to  
 10 Plaintiffs and the Class Members as reasonable consumers. Had Plaintiffs and the Class Members  
 11 known of Costco's unlawful conduct, they would not have interacted with its Website, including,  
 12 for example, by purchasing prescriptions through its Website, nor relied on its health care  
 13 services, or they would have demanded compensation for such data sharing.

14       167. Moreover, Plaintiffs and the Class Members have been deprived of the value  
 15 inherent in their personal information that Defendant unlawfully disclosed to third parties. A  
 16 market exists for the collection of patient data, including an individual's personal, health, and  
 17 financial information, and companies will—and must—pay a premium to obtain this valuable  
 18 commodity. Accordingly, Plaintiffs and the Class Members have a property interest in their  
 19 private information and thus were deprived of appropriate consideration and compensation for  
 20 the unauthorized data-sharing with third parties of Plaintiffs' and the Class Members' private and  
 21 protected communications without consent or consideration.

22       168. Defendant's conduct is unfair as it offends public policy as established by statute  
 23 and is otherwise unethical, oppressive, or unscrupulous.

24       169. There is a causal link between the unfair and deceptive acts complained of and  
 25 the injuries alleged.

170. Plaintiffs and the Class Members are entitled to damages, statutory treble damages, and reasonable attorneys' fees under Washington Revised Code Section 19.86.090.

**COUNT IV**

## **Violation of the Washington Uniform Health Care Information Act (“UHCIA”)**

## **Wash. Rev. Code. § 70.02 et seq.**

**(By Plaintiffs and on behalf of the Nationwide Class)**

171. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

172. The Washington Uniform Health Care Information Act (“UHCIA”) defines a “health care provider” as “a person who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession.” Wash. Rev. Code § 70.02.010(19).

173. The UHCIA defines “health care” as “any care, service, or procedure provided by a health care provider,” including “[t]o diagnose, treat, or maintain a patient’s physical or mental condition; or [t]hat affects the structure or any function of the human body.” *Id.* § 70.02.010(15).

174. Costco is a “health care provider” under the UHCIA because it is authorized to provide health care services, including pharmaceutical services, and it provides care and services that treat a patient’s physical or mental condition and that affects the structure or functions of the human body, including, for example, the sale and dispensing of prescription drugs used in the treatment of a patient’s physical or mental health or medical condition.

175. Plaintiffs and the Class Members are “patients” at all relevant times as that term is defined under the UHCIA because they are “individual[s] who receive[] or ha[ve] received health care.” *Id.* § 70.02.010(34).

176. In addition, the UHCIA defines “health care information” as “any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient’s health care” and “includes any required accounting of disclosures of health care information.” *Id.* § 70.02.010(17).

1       177. The information Plaintiffs and the Class Members communicated with Defendant  
 2 on its Website concerned the past, present, and future physical or mental health or condition and  
 3 the provision of health care. This information directly relates to a patient's health care and can  
 4 be identified, or can be readily associated with the identity of, a patient. Thus, that information  
 5 constitutes "health care information" as that term is defined in the UHCIA.

6       178. Under the UHCIA, it is unlawful for a third party to access a patient's health care  
 7 records from a provider, or a person who receives records from a provider, without the patient or  
 8 the patient's legally authorized representative's consent, specific authorization in law, or a  
 9 representative from a provider that holds a signed and dated consent from the patient authorizing  
 10 the release. *Id.* §§ 70.02.020(1), 70.02.030(1), (3)–(4).

11       179. Under the UHCIA, it is unlawful for a health care provider, its agents, employees,  
 12 and those who assist a health care provider in the delivery of health care to "disclose health care  
 13 information about a patient to any other person without the patient's written authorization." *Id.* §  
 14 70.02.020(1).

15       180. The UHCIA further prohibits a health care provider to "use or disclose health care  
 16 information for marketing" or "[s]ell health care information to a third party" without the  
 17 patient's authorization. *Id.* §§ 70.02.280(1) & (2)(h).

18       181. Defendant's use of Meta Pixel resulted in Defendant disclosing to a third party  
 19 Plaintiffs' and the Class Members' health care information and, furthermore, allowed a third  
 20 party to access, without authorization, Plaintiffs' and the Class Members' health care  
 21 information.

22       182. Neither Plaintiffs nor the Class Members consented to or otherwise authorized  
 23 Defendant to share their private health care information with Meta or any other third party. Under  
 24 the UHCIA, a health care provider or other person who causes an unauthorized release of health  
 25 care information by disclosing such information in violation of the UHCIA shall be subject to  
 26 suit and may be liable to the patient for compensatory damages, plus costs and reasonable

1 attorneys' fees. *Id.* § 70.02.170(1)–(2). As a result of Defendant's violations of the UHCIA,  
 2 Plaintiffs and the Class Members seek all damages authorized by law, including compensatory  
 3 damages, plus costs and reasonable attorneys' fees.

4 **COUNT V**

5 **Invasion of Privacy**  
 (By Plaintiffs and on behalf of the Nationwide Class)

6 183. Plaintiffs reallege and incorporate by reference every allegation contained in the  
 7 paragraphs above as though fully set forth herein.

8 184. Washington common law recognizes the tort of invasion of privacy. The right to  
 9 privacy is also established in the Constitution of the State of Washington which explicitly  
 10 recognizes an individual's right to privacy and states under Article 1, Section 7: "No person shall  
 11 be disturbed in his private affairs, or his home invaded, without authority of law."

12 185. A claim for intrusion on seclusion requires (1) an intentional intrusion, physically  
 13 or otherwise, (2) upon the solitude or seclusion of another or his private affairs or concerns, and  
 14 (3) the intrusion must be highly offensive to a reasonable person.

15 186. Plaintiffs and the Class Members have an objective, reasonable expectation of  
 16 privacy in browsing sessions conducted on their personal devices and their highly personal and  
 17 private Sensitive Information, including their patient status, prescription and immunization  
 18 information, health insurance information, and other highly sensitive data.

19 187. Defendant's conduct, through its unlawful embedding of Pixel and subsequent  
 20 interception, recording, and unauthorized disclosure of Plaintiffs' and the Class Members'  
 21 private communications regarding sensitive health information when they visited and interacted  
 22 with Defendant's Website without their consent, violates Article 1, Section 7 of the Constitution  
 23 of the State of Washington.

24 188. Plaintiffs and the Class Members did not consent to, authorize, or know about  
 25 Defendant's intrusion at the time it occurred. Plaintiffs and the Class Members never agreed that  
 26 Defendant could install a recording device (Pixel or other tracking technologies) to actively

1 record their Website Communications in real-time or disclose their private communications and  
 2 sensitive health information to Defendant's vendors or other third parties.

3       189. Plaintiffs and the Class Members have a legitimate, objective, and reasonable  
 4 expectation of privacy in private browsing sessions and precluding the dissemination and/or  
 5 misuse of their highly sensitive health information and private communications and in  
 6 conducting their personal activities without intrusion or interference, including the right to not  
 7 have their personal information intercepted and utilized for commercial gain.

8       190. By intentionally embedding and implementing the tracking technologies on its  
 9 Website, Defendant intruded upon, and permitted unauthorized third parties to intrude upon,  
 10 Plaintiffs' and the Class Members' private communications with Defendant regarding their  
 11 sensitive health information without consent.

12       191. Defendant's use of Pixel also resulted in the publication of Plaintiffs and Class  
 13 Members' private affairs to another in a manner that is highly offensive to a reasonable person.  
 14 As a result of Defendant's use of the Pixel, Plaintiffs' and Class Members sensitive health  
 15 information was transmitted to one of the largest advertising companies in the world for purposes  
 16 of creating targeted advertising and marketing campaigns.

17       192. Defendant's secret use of Pixel and other tracking technologies to record and  
 18 disclose Plaintiffs' and the Class Members' Sensitive Information obtained via the Website is  
 19 highly offensive and objectionable to a reasonable person and constitutes an egregious breach of  
 20 the social norms underlying the right to privacy given the sensitive nature of the health  
 21 information and state and federal statutes prohibiting disclosure of such information.

22       193. Defendant's conduct, by secretly and unlawfully intercepting, and permitting the  
 23 unauthorized third-party use of, Plaintiffs' and the Class Members' communications any time  
 24 they interacted with Defendant's Website with Pixel enabled without their consent, was a  
 25 proximate cause of damage to Plaintiffs and the Class Members. Plaintiffs and the Class have  
 26

suffered losses of privacy, loss of control of their private data, and a diminution of value of their personal information.

194. Additionally, given the monetary value of individual personal information, Defendant deprived Plaintiffs and the Class Members of the economic value of their interactions with Defendant's Website, without providing proper consideration for Plaintiffs' and the Class Members' property.

195. Further, Defendant has improperly profited from its invasion of Plaintiffs' and the Class Members' privacy in its use of their data for its economic value.

196. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class Members are entitled to damages, including compensatory, and/or nominal damages, in an amount to be proven at trial.

**COUNT VI**  
**Breach of Implied Contract**  
**(By Plaintiffs and on behalf of the Nationwide Class)**

197. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

198. When Plaintiffs and Class Members paid money and provided their Sensitive Information to Defendant in exchange for services, they entered implied contracts pursuant to which Defendant agreed to safeguard and not disclose their Sensitive Information without Plaintiffs' and Class Members' consent.

199. An implicit part of the agreement was that Defendant would safeguard Plaintiffs' and Class Members' Sensitive Information consistent with industry and regulatory standards and Defendant's privacy policy and would timely notify Plaintiffs in the event of a disclosure to third parties.

200. Plaintiffs and Class Members would not have entrusted Defendant with their Sensitive Information in the absence of an implied contract between them and Defendant obligating Defendant not to disclose this information without consent.

201. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

202. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Sensitive Information to various third parties, including Meta.

203. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their sensitive health-related information would be disclosed.

204. Plaintiffs and Class Members are entitled to compensatory and consequential damages because of Defendant's breaches of implied contract.

## COUNT VII

## Conversion

**(By Plaintiffs and on behalf of the Nationwide Class)**

205. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

206. Plaintiffs and the Class Members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare-related information and knowledge. This Sensitive Information was the personal property of Plaintiffs and the Class Members.

207. Defendant converted Plaintiffs' and Class Members' Sensitive Information by willfully misappropriating and misusing the Sensitive Information for marketing purposes, which was not the intended purpose of Plaintiffs and Class Members in providing the personal information to Defendant

208. Defendant's unlawful conversion interfered with and deprived Plaintiffs' and Class Members' of their possessory interests in their Sensitive Information by causing Plaintiffs and Class Members to lose control over the dissemination of their personal medical data, which was intended only for Defendant.

209. Plaintiffs' and Class Members' possessory rights in their Sensitive Information were seriously impaired by Defendant's intentional misuse and disclosure of their information to unauthorized third parties, from which Plaintiffs and Class Members have no ability recover their Sensitive Information.

210. As a direct and proximate result of Defendant's conversion, Plaintiffs and Class Members suffered the loss of their Sensitive Information and are entitled to damages, including compensatory and/or nominal damages, in an amount to be proven at trial.

**COUNT VIII**  
**Unjust Enrichment**  
**(By Plaintiffs and on behalf of the Nationwide Class)**

211. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

212. Plaintiffs and the Class Members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare-related information and knowledge. Defendant knowingly and unlawfully received a benefit from its use of Plaintiffs' and the Class Members' Sensitive Information, including monetary compensation. Defendant intentionally and knowingly collected and used Plaintiffs' and the Class Members' Sensitive Information for its own gain, without Plaintiffs' or the Class Members' consent, authorization, or compensation.

213. Defendant unjustly retained those benefits and enriched itself at the expense of Plaintiffs and the Class Members, and this conduct damaged Plaintiffs and the Class Members. Plaintiffs and the Class Members were not compensated by Defendant for the data they unknowingly provided.

214. It would be inequitable and unjust for Defendant to retain any of the profit or other financial benefits derived from the secret, unfair, and deceptive data harvesting methods Defendant employs on its Website.

215. The Court should require Defendant to disgorge all unlawful or inequitable proceeds that it received into a common fund for the benefit of Plaintiffs and the Class Members, and order other such relief as the Court may deem just and proper.

216. Plaintiffs allege this claim in the alternative in the event Plaintiffs and Class Members have an inadequate remedy at law.

## **REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

- a. Certification of the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;
  - b. Designation of Plaintiffs as representatives of the Class and the undersigned counsel as Class Counsel;
  - c. An award of damages in an amount to be determined at trial or by this Court;
  - d. Declaring that Defendant's past conduct was unlawful, as alleged herein;
  - e. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
  - f. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
  - g. Awarding Plaintiffs and the Class Members statutory, actual, compensatory, consequential, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
  - h. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest;
  - i. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and
  - j. Granting such other relief as the Court deems just and proper.

1                   **DEMAND FOR JURY TRIAL**

2                   Plaintiffs, on behalf of themselves and the Class, demand a trial by jury of any and all  
3 issues in this action so triable of right.

4                   DATED this 6th day of October, 2023.

5                   TOUSLEY BRAIN STEPHENS PLLC

7                   By: s/ Kim D. Stephens, P.S.  
8                   Kim D. Stephens, P.S., WSBA #11984

9                   By: s/ Rebecca L. Solomon

10                  Rebecca L. Solomon, WSBA #51520  
11                  1200 Fifth Avenue, Suite 1700  
12                  Seattle, WA 98101  
13                  Telephone: (206) 682-5600  
14                  Facsimile: (206) 682-2992  
15                  kstephens@tousley.com  
16                  rsolomon@tousley.com

17                  **ZIMMERMAN REED LLP**

18                  By: s/Ryan J. Ellersick  
19                  Ryan J. Ellersick, WSBA # 43346  
20                  Hart L. Robinovitch\*  
21                  14648 North Scottsdale Road, Suite 130  
22                  Scottsdale, AZ 85254  
23                  Telephone: (480) 348-6400  
24                  ryan.ellersick@zimmreed.com  
25                  hart.robinovitch@zimmreed.com

26                  \* *Pro Hac Vice applications to be submitted*

27                  *Attorneys for Plaintiffs and the Putative Class*